Vysoká škola báňská – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Paketové analyzátory

Packet analyzers

2016

Tomáš Stiborský

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání bakalářské práce

Student: **Tomáš Stiborský**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2601R013 Telekomunikační technika

Téma: Paketové analyzátory
Packet Analysers

Jazyk vypracování: čeština

Zásady pro vypracování:

Cílem bakalářské práce je srovnání různých paketových analyzátorů a jejich otestování v různých typech počítačových sítí a pro různé formy komunikace. Výsledkem práce bude zhodnocení předností a nedostatků jednotlivých paketových analyzátorů.

Osnova práce:
1. Popište paketové analyzátory, které se v současnosti používají.
2. Popište a prakticky otestujte některé speciální funkce vybraných paketových analyzátorů.
3. Srovnejte výhody a nevýhody jednotlivých paketových analyzátorů.

Seznam doporučené odborné literatury:

{1] SANDERS, Chris. *Analýza sítí a řešení problémů v programu Wireshark.* Brno: Computer Press, 2012. ISBN 978-80-251-3718-5.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Petr Machník, Ph.D.**

Datum zadání: 01.09.2015

Datum odevzdání: 29.04.2016

VYSOKÁ ŠKOLA BÁŇSKÁ - TECHNICKÁ UNIVERZITA OSTRAVA * Fakulta elektrotechniky a informatiky * OSTRAVA *

doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě 24. dubna 2016 .....

Děkuji panu Ing. Petru Machníkovi, Ph.D. za cenné rady, trpělivost a odborné vedení při zpracování mé bakalářské práce.

Abstrakt

Práce poskytuje popis funkcí paketových analyzátorů Wireshark, TCPDUMP, Microsoft Network Monitor, Colasoft Capsa a BitShark společně s náhledem grafického zpracování těchto analyzátorů. V práci lze nalézt praktické ukázky a návody využití speciálních funkcí analyzátorů Wireshark a Colasoft Capsa. Jako speciální funkce Wiresharku je popsána analýza rámců 802.11, zachytávání na vzdáleném rozhraní, analýza VoIP hovorů a tvorba I/O grafů. Dále práce obsahuje návod na využití analyzátoru Colasoft Capsa a jeho nástrojů k DoS útoku na vybrané zařízení v síti, návod na tvorbu alarmů a grafů pomocí tohoto analyzátoru. Závěrem práce je srovnání popisovaných analyzátorů po stránce vizuální, finanční, po stránce složitosti používání a podpory operačních systémů.

Klíčová slova: analýza 802.11, analýza sítě, analýza VoIP, BitShark, Colasoft Capsa, DoS útok, graf síťového provozu, Microsoft Network Monitor, paketový analyzátor, TCPDUMP, vzdálené zachytávání, Wireshak

Abstract

The work provides a description of the functions of packet analyser Wireshark, TCPDUMP, Microsoft Network Monitor, Colasoft Capsa and BitShark along with a preview of the graphic design of these analysers. At work, we can find practical examples and tutorials to use special function from Wireshark and Colasoft Capsa. As a special feature of Wireshark is described 802.11 frame analysis, capturing the remote interface, analysis of VoIP calls and creation of I / O graphs. The work also includes instructions on using the analyser Colasoft Capsa and its tools for DoS attacks on selected devices in the network, instructions for creating graphs and alarms using this analyser. In conclusion compares graphical design, financially, complexity of the applications and operating system support of described analysers.

Keywords: analysis of 802.11, analysis VoIP, BitShark, Colasoft Capsa, DoS atack, Microsoft Network Monitor, network analysis, network trafic graph, packet analyser, remote capture, TCPDUMP, Wireshark

Seznam použitých zkratek a symbolů

ARP	–	Address Resolution Protocol
DoS	–	Denial of Service
DNS	–	Domain Name System
FTP	–	File Transfer Protocol
HTML	–	Hyper Text Markup Language
HTTP	–	Hyper Text Transport Protocol
ICMP	–	Internet Control Message Protocol
IPv4	–	Internet Protocol version 4
IPv6	–	Internet Protocol version 6
LDAP	–	Lightweight Directory Access Protocol
MAC	–	Media access control address
MNM	–	Microsoft Network Monitor
MSD	–	Berkeley Software Distribution
MTU	–	Maximum Transmission Unit
OSI	–	Open Systems Interconnection
POP	–	Post Office Protocol
RADIUS	–	Remote Authentication Dial-In User Service
RFC	–	Requests for Comments
RM	–	Referenční model
RPCAPD	–	Remote Packet Capcure Prococol
SIP	–	Session Initiation Protocol
SMB	–	Server Message Block
SSH	–	Secure Shell
TCP	–	Transmission Control Protocol
UDP	–	User Datagram Protocol
VoIP	–	Voice Over Internet Protocol

Obsah

Seznam obrázků

Úvod

Tato bakalářská práce pojednává o softwaru, jenž dokáže zachytit síťový provoz, následně dekóduje a implementuje binární data do podoby čitelné pro člověka. Tento software se nazývá paketovým analyzátorem. První kapitola poskytne uživateli kroky, kterými se řídit při výběru paketového analyzátoru. Následně vysvětlí obecný princip práce tohoto programu. Nakonec nastíní síťové topologie, které může síťový analytik řešit, a jakým způsobem se dají v sítích data zachytávat.

Druhá kapitola poskytuje přehled o funkcích a grafickém zpracování nejznámějších paketových analyzátorů pro nejrozšířenější operační systémy Linux, Windows a Android. Analyzátory Wireshark a TCPDUMP jsou zde popsány jako zástupci mutiplatformních analyzátorů, které jsou k dispozici zdarma. Zástupcem podnikového řešení paketového analyzátoru pro systém Windows je zde analyzátor Colasoft Capsa. Další analyzátor, popisován pro systém Windows, je Microsoft Network Monitor. Posledním vybraným analyzátorem je BitShark, jenž zastupuje analyzátory pro platformu Android. V kapitole lze nalézt náhled zpracování nejpoužívanějších analytických vlastností jednotlivých analyzátorů společně s návodem, jak danou funkci v analyzátoru najít.

Obsahem třetí kapitoly jsou ukázky speciálních funkcí analyzátorů Wireshark a Colasoft Capsa. V kapitole lze najít řešení problému zachytávání bezdrátového provozu pomocí emulace síťové karty AirPcap pro analyzátor Wireshark. Dále poskytuje podrobný návod, jak využít Wireshark k analýze provozu ze vzdáleného rozhraní. Také lze najít ukázku a návod k dekódování VoIP, grafu toku dat, či tvorbu grafů.

Z analyzátoru Colasoft Capsa jsou zde popsány nástroje MAC Scaner, Ping Tool, Packet Builder, Packet Player společně s ukázkou, jak je využít k DoS útoku na vybrané zařízení v síti. Závěrem kapitoly je ukázka funkce alarm a tvorba grafů.

Poslední kapitola srovnává uvedené analyzátory po stránce vizuální, finanční, po stránce složitosti používání a podpory operačních systémů.

1 Nástroje pro sledování paketů

Analýza paketů, která se často označuje jako sledování paketů (packet sniffing), popisuje proces zachytávání a interpretace aktuálních dat přenášených v síti. Díky tomu lze lépe porozumět fungování dané sítě, zároveň ale poskytuje příležitost pro útočníka - ten může zneužít obsah těchto dat ve svůj prospěch. K analýze paketů se obvykle používá paketový analyzátor, který umožňuje zachytávat neformátovaná síťová data při jejich přenosu. K dispozici jsou analyzátory různých typů a vlastností včetně bezplatných a komerčních podnikových řešení. [11, str.20]

1.1 Hodnocení paketového snifferu

Při výběru paketového zachytávače je nutné zohlednit několik faktorů:

- **Podporované protokoly** - Všechny paketové analyzátory umožňují interpretovat více protokolů. Většina z nich dokáže interpretovat běžné síťové protokoly (např. IPv4, ICMP), protokoly transportní vrstvy (např.TCP a UDP) a dokonce protokoly aplikační vrstvy (např. DNS, HTTP). Nemusí však podporovat novější protokoly (např. IPv6, SIP). Před nasazením paketového analyzátoru musíme ověřit, zda je kompatibilní s protokoly, které chceme analyzovat.

- **Snadné používání** - Vezměme v úvahu uspořádání ovládacích prvků programu, snadnost instalace a celkové postupy starndardních operací. Zvolený program by měl odpovídat úrovni znalostí uživatele.

- **Náklady** - Výhodou paketových analyzátorů je, že existuje mnoho bezplatných programů, které jsou srovnatelné s kterýmkoli komerčním produktem. Komerční produkty a jejich bezplatně dostupné alternativy se liší zejména svými vykazovacími moduly. Komerční programy obvykle obsahují nějaký modul na vygenerování složitých výkazů, jež má u bezplatných aplikací často jen omezené možnosti nebo úplně chybí.

- **Podpora programu** - Když porovnáme dostupnou podporu, všímáme si dostupné dokumentace, veřejných fór a e-mailových konferencí. Bezplatné programy obvykle neposkytují podporu vývojářů, ale tuto mezeru často zaplňují komunity uživatelů daných aplikací. Komunity uživatelů a přispěvovatelů provozují diskuzní fóra, wiki či blogy, kde můžeme získat dostatek námi požadovaných informací.

- **Podpora operačních systémů** - Některé paketové analyzátory nejsou kompatibilní se všemi operačními systémy. Musíme volit program, který bude kompatibilní s operačním systémem, jež budeme používat.

  [11, str.20,21]

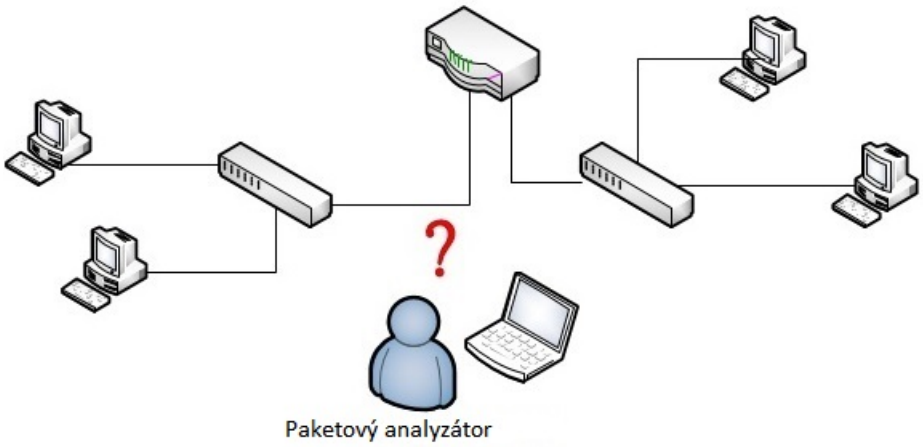
1.2 Principy paketových analyzátorů

Proces sledování paketů vyžaduje spolupráci softwaru a hardwaru. Celý proces lze rozdělit na tři fáze: [11, str.21]

- **Shromažďování** - V prvním kroku paketový analyzátor sbírá neformátovaná binární data, která putují po síti. Přitom se vybrané síťové rozhraní obvykle přepíná do promiskiutního režimu. V tomto režimu dokáže síťová karta naslouchat veškerému provozu v síťovém segmentu, nikoli pouze datům, krerá jsou jí adresována.
- **Konverze** - V tomto kroku jsou zachycená binární data převedena do čitelného tvaru. Zde končí možnosti většiny pokročilých paketových analyzátorů pro příkazový řádek. V této fázi mají síťová data podobu, kterou lze inpretetovat pouze na základní úrovni. Větší část analýzy je na uživateli.
- **Analýza** - Třetí a závěrečný krok zahrnuje vlastní analýzu zahlcených a kovertovaných dat. Paketový analyzátor načte zachycená síťová data, na základě extrahovaných informací zkontroluje síťové protokoly a zahájí analýzu konkrétních vlastností příslušného protokolu.

1.3 Prostředí pro sledování

Přepokladem efektivní analýzy paketu je rozhodnutí o tom, kde umístit počítač s paketovým analyzátorem, aby učinně zachytával data. Při sledování síťových paketů nestačí pouze připojit notebook k síťovému portu a začít se zachytáváním provozu. V praxi je umístění paktového zachytávače do síťové kabeláže často obtížnější než samotná analýza paketů (viz Obrázek 1.1.) Problém se zapojením zachytávače spočívá v tom, že se k propojení zařízení používá mnoho různých komponent (přepínače, směrovače, rozbočovače). Jelikož se tato zařízení liší ve způsobu zpracování provozu, je třeba dopředu znát fyzickou topologii. [11, str.35]



Obrázek 1.1: Umístění zachytávače bývá problematické [11, str.36]

1.3.1 Promiskuitní režim

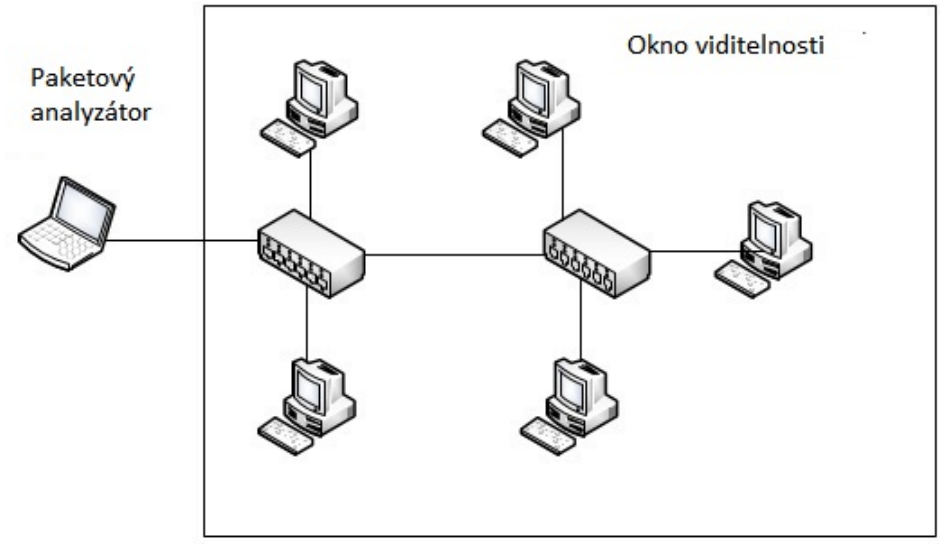
Jednou z vlastností síťové karty je zahazování rámců, jež jí nejsou adresovány, aniž by je předala ke zpracování procesoru. Ve velkém síťovém provozu by bylo neefektivní, kdyby všechny klientské stanice zpracovávaly veškerý provoz, jež jim není určen. Síťová karta rozezná, že jí paket není určen a ihned ho zahodí. Díky tomu šetří výpočetní výkon procesoru.

Zahazování paketů zlepšuje efektivitu zpracování, ale z hlediska analýzy tato vlastnost není příliš vhodná. Pro účel síťové analýzy chceme zachytit každý paket odeslaný na lince, aby nám neunikla některá klíčová informace.

Zachycení veškerých dat lze dosáhnout pomocí promiskuitního režimu síťové karty. Síťová karta v promiskuitním režimu předává procesoru každý paket bez ohledu na to komu je adresován. Jakmile je paket předán pro zpracování procesoru, můžeme využít aplikaci pro sledování paketů. Proto je nutné, aby síťová karta podporovala ovladač pro přechod do promiskuitního režimu. Většina dnešních síťových karet tuto možnost podporuje a paketové analyzátory umí kartu přepnout do promiskuitního režimu přímo z grafického rozhraní. [11, str.35,36]

1.3.2 Sledování s rozbočovači

Rozbočovač funguje na nejnižší vrstvě RM/OSI modelu. Přijatá data z jednoho portu odesílá na všechny své porty, proto ke sledování stačí připojit zachytávač do volného portu rozbočovače. Jak ukazuje Obrázek 1.2, okno viditelnosti není při sledování s rozbočovači nijak omezeno. Užití rozbočovačů v síti má však nevýhodu vzniku kolize v situacích, kdy začne vysílat data více stanic současně. [11, str.37]

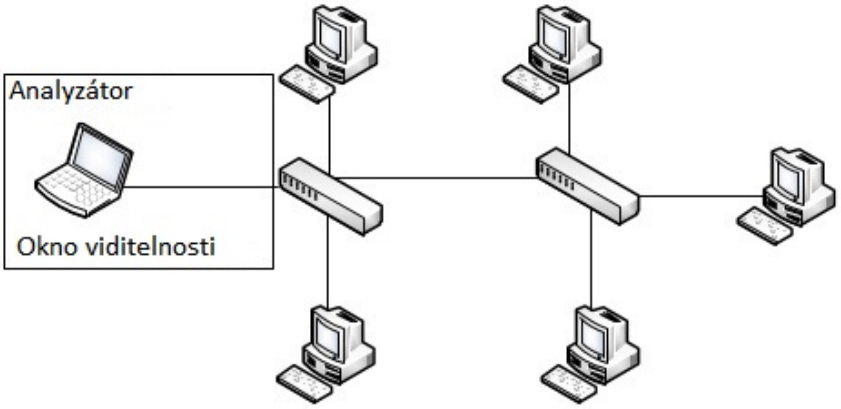


Obrázek 1.2: Sledování v síti s rozbočovači [11, str.37]

1.3.3 Sledování v přepínaném prostředí

Přepínač pracuje na druhé vrstvě RM/OSI. To umožňuje data v síti adresovat a posílat pouze na určitý port, kde je připojeno cílové zařízení. Kromě toho umožňuje zařízení duplexní komunikaci, tzn. počítače mohou data vysílat a přijímat v jeden okamžik. Z hlediska analýzy paketů výrazně zvyšují úroveň složitosti. Jak ukazuje obrázek 1.3, sledování je omezeno pouze na všesměrový provoz a provoz odesílaný či přijímaný svým vlastním zařízením.

Pokud chceme zachytávat provoz z cílového zařízení v přepínané síti, můžeme využít jednu ze čtyř primárních metod: Zrcadlení portu, rozbočování, použití odposlechu a znehodnocení mezipaměti ARP. [11, str.38]



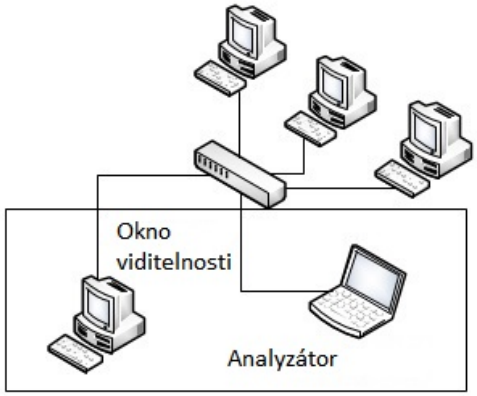
Obrázek 1.3: Okno viditelnosti je omezeno na port, kde je zachytávač připojen [11, str.39]

- **Zrcadlení portu** (port mirroring) představuje snad nejjednodušší způsob, jak zachytávat provoz cílového zařízení v přepínané síti. Přepínač musí podporovat funkci zrcadlení portu a musí mít jeden volný port pro připojení zachytávače.

  Chceme-li zapnout zrcadlení portu, zadáme příkaz, který nařídí přepínači kopírovat veškerý provoz z vybraného portu na port jiný. Některá zařízení podporují zrcadlení z více portů, což je užitečné při analýze komunikace mezi více zařízeními. Analýza pomocí zrcadlení portu je velice efektivní z hlediska selektivity sledovaných zařízení (viz Obrázek 1.4.). [11, str.39,40]

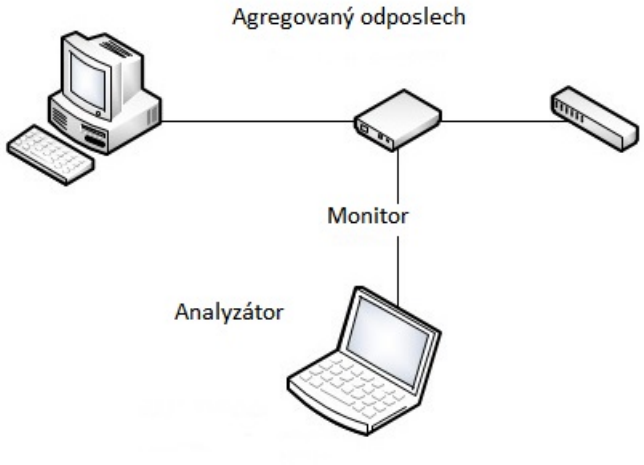
- **Rozbočování** je metoda, při níž využíváme vlastností rozbočovače. Metoda spočívá v přípojení zachytávače spolu se sledovaným zařízením do stejného síťového segmentu pomocí rozbočovače. [11, str.40,41]

- **Použití odposlechu** - síťový odposlech je hardwarové zařízení, které můžeme umístit mezi dva body v kabeláži. Síťové odposlechy dělíme na dva základní druhy: Agregované a neagregované. [11, str.42]



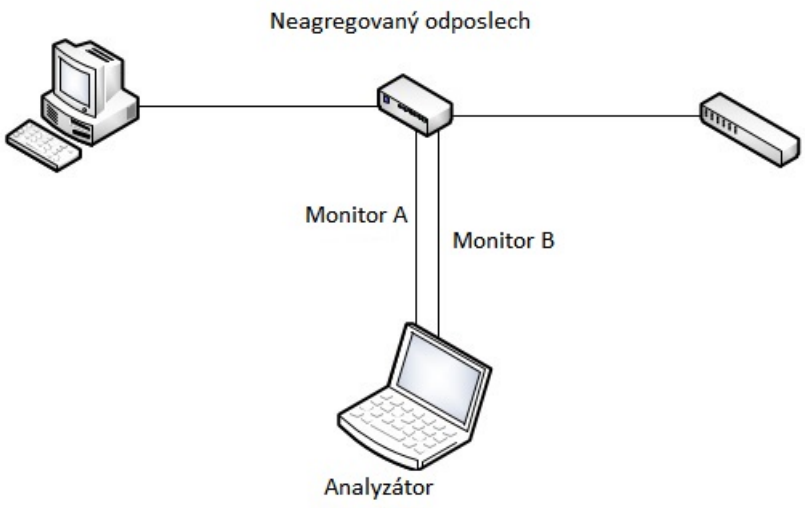
Obrázek 1.4: Zrcadlení nám umožní výběr sledovaného zařízení

Agregovaný odposlech má tři porty: vstupní, výstupní a pro oba směry provozu jeden společný monitorovací port (viz Obrázek 1.5.).



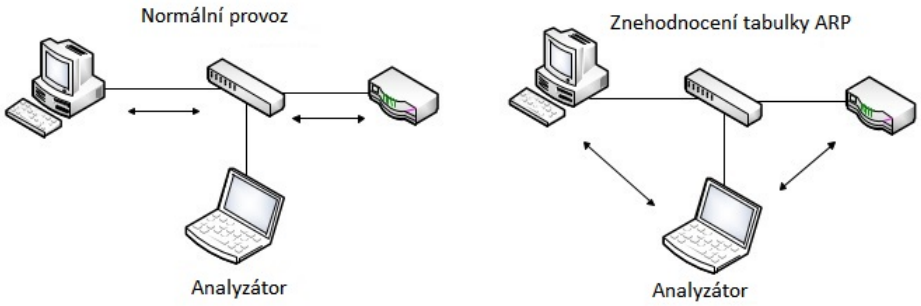
Obrázek 1.5: Zachytávání provozu pomocí agregovaného odposlechu [11, str.43]

Neagregovaný odposlech má čtyři porty a poskytuje poněkud vyšší pružnost při zachytávání provozu. Dva z portů slouží jako vstup a výstup, přičemž další dva jsou monitorovací - každý pro jeden směr komunikace. Nevýhodou je potřeba dvou síťových karet, které nám zároveň poskytují výhodnou možnost zachytávání vyšší přenosovou rychlostí, jež je při agregovaném odposlechu sdílena na jedné lince. [11, str.43,44]



Obrázek 1.6: Zachytávání provozu pomocí neagregovaného odposlechu [11, str.44]

- **Znehodnocení mezipaměti ARP**, které se také někdy označuje jako falšování ARP (ARP spoofing), je založeno na odesílání speciálních zpráv ARP ethernetovému přepínači nebo směrovači. V těchto zprávách falzifikujeme MAC adresu tak, aby záznamy v ARP tabulkách sledovaných zařízení podvrhli informaci, že naš zachytávač je výchozí router. Analogicky je v ARP tabulkách routeru náš zachytávač uložen jako cílové zařízení (viz Obrázek 1.7) .[11, str.45,46]



Obrázek 1.7: Změna průběhu komunikace při znehodnocení ARP [11, str.46]

2 Používané paketové analyzátory

Jelikož síťový provoz nám vytváří nespočet problémů a situací, k jejímž řešením je třeba použít specifický analyzátor, uvedeme si z velkého množství dnes dostupných analyzátorů zástupce, jež by bylo v danných situacích vhodné použít.

2.1 TCPDUMP

Paketový analyzátor TCPDUMP je nejznámější analyzátor v příkazové řádce. Je pouze textového charakteru a veškerá analýza je hlavně na zkušenostech uživatele. Díky textovému charakteru a minimální náročnosti je možné tento analyzátor používat vzdáleně přes Telnet nebo SSH. Další výhodou je jeho malá náročnost na paměť a implementaci samotného analyzátoru, díky tomu je TCPDUMP dnes dostupný pro všechny operační systémy. Na Linuxu jej můžete naistalovat pomocí příkazu "sudo apt-get install tcpdump". Pro windows má TCPDUMP verzi s názvem WINDUMP dostupný zde: [8] Jeho textová forma je zároveň nevýhodou, jelikož neumožňuje hlubší analýzu a rozbor dat, jako je tomu u analyzátorů s grafickým rozhraním.

Ukázková situace užití TCPDUMP

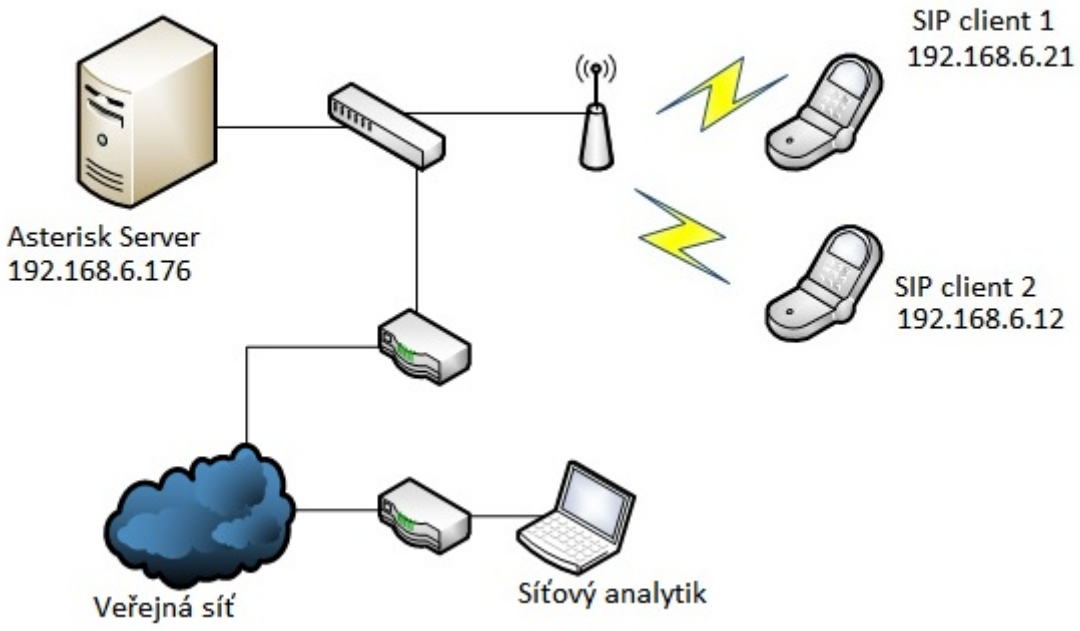
Malá firma pro své hovory používá VoIP telefonii. Jelikož v době chytrých telefonů není problém nainstalovat aplikaci SIP clienta na kterýkoli telefon, zaměstnanci kromě pevného telefonu v kanceláři mohou využívat vlastní chytrý telefon připojený k firemní síti pomoci bezdrátové sítě wifi. Jeden ze zaměstnanců si stěžuje na problémy s přihlášením k serveru. Správce sítě v administraci serveru Asterisku nenachází chybu. Proto potřebuje vidět pakety putující mezi telefony a serverem. Jelikož je mimo firmu na služební cestě, jediný způsob, jak data analyzovat, je spustit analyzátor přes SSH přímo na serveru. Obrázek 2.1 naznačuje situaci připojení administátora.

V případě potřeby přihlášení k serveru z linuxu stačí napsat do terminálu příkaz ssh login@ip-adresa-serveru, u windows systému je nejjednodušší přihlášení pomocí programu Putty dostupného z odkazu [14].

Okno putty má jednoduché a snadné rozhraní pro uživatele. K připojení nám stačí zakliknout možnost SSH, vyplnit IP adresu serveru a kliknout na tlačítko open. V obou případech potvrdíme důvěryhodnost serveru a povolíme výměnu privátního klíče pro šifrování dat.

Po nainstalování TCPDUMPU jej spustíme příkazem tcpdump + filtrační parametry. Příkladem může být příkaz "tcpdump -i any -n port 5060", kde parametr "-i any"značí zachytávání ze všech rozhraní, parametr "-n"vypíná překládání doménových jmen, abychom viděli pouze IP adresy, a poslední parametr - port 5060 - filtruje pouze provoz na portu 5060, kde komunikují telefony se SIP serverem. Jak ukazuje Obrázek 1.2, v rámci tohoto filtru je pro nás nová informace pouze zdrojový port a adresa zařízení komuninikujících se serverem.

Přidáním parametru "-w NazevSouboru.cap"zachycená data analyzátor ukládá do souboru. Soubor můžeme po ukončení zachytávání stáhnout a zobrazit v jiném grafickém analyzátoru nebo otevřít zpětně pomocí parametru "-r"(tcpdump -r /cestaksouboru/NazevSouboru.cap). Parametr "-v"slouží k dekódování paketů a zobrazení podrobnějších



Obrázek 2.1: Schéma situace v síti

```
root@bananapi ~ # tcpdump -i any -n  port 5060
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 65535 bytes
18:34:39.444772 IP 192.168.6.176.5060 > 192.168.6.12.47705: SIP, length: 548
18:34:39.755079 IP 192.168.6.12.47705 > 192.168.6.176.5060: SIP, length: 1043
18:35:00.639420 IP 192.168.6.12.47705 > 192.168.6.176.5060: SIP, length: 2
18:35:03.311385 IP 192.168.6.21.57063 > 192.168.6.176.5060: SIP, length: 580
18:35:03.406512 IP 192.168.6.176.5060 > 192.168.6.21.57063: SIP, length: 560
18:35:03.458533 IP 192.168.6.21.57063 > 192.168.6.176.5060: SIP, length: 744
```

Obrázek 2.2: Zachycené pakety na Asterisku

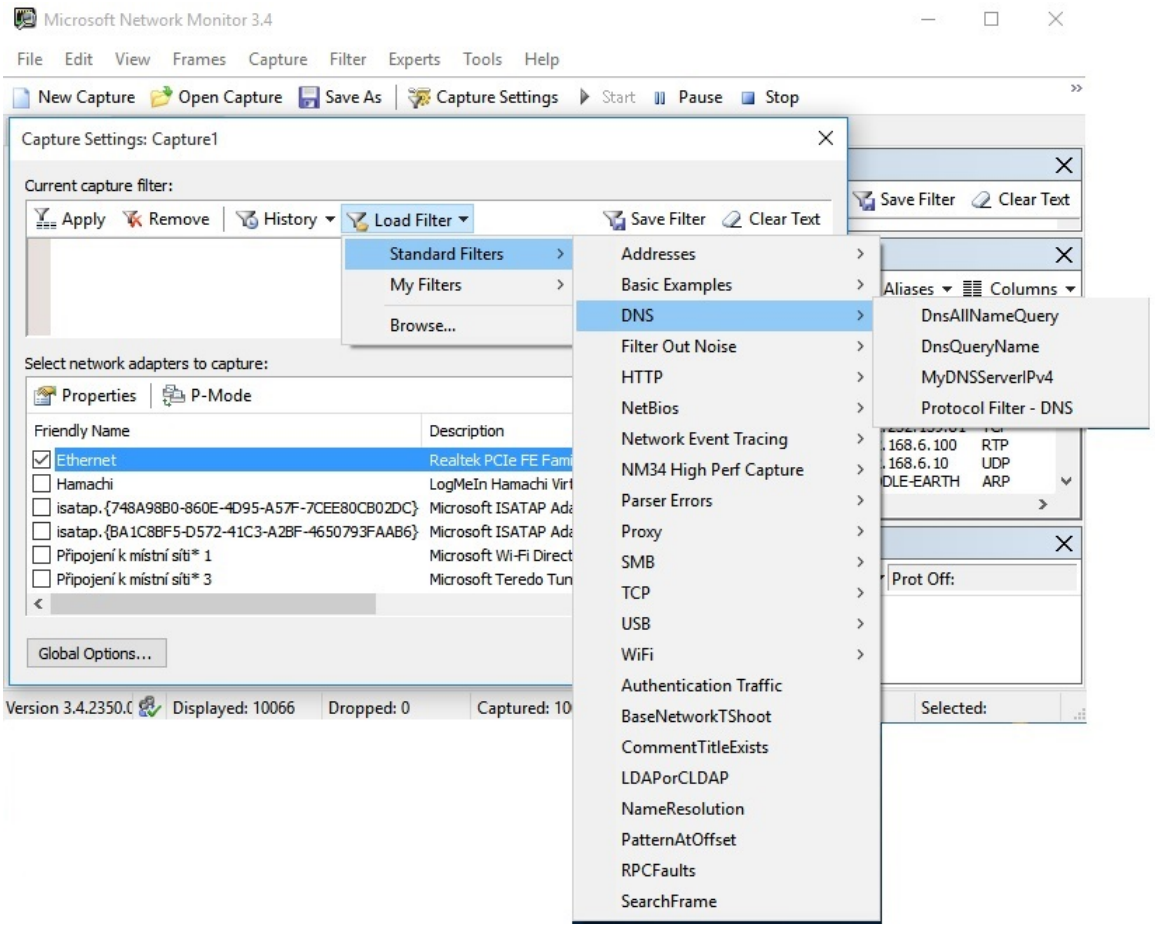
informací (viz Obrázek 2.3.). Parametrem -vv přidáme k výpisu i originální hexadecimální podobu dat.

```
root@bananapi ~ # tcpdump -i any -n  port 5060 -v
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked), capture size 65535 bytes
19:20:53.252435 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 555)
    192.168.6.12.47705 > 192.168.6.176.5060: SIP, length: 527
        REGISTER sip:192.168.6.176:5060 SIP/2.0
        Via: SIP/2.0/UDP 192.168.6.12:47705;rport;branch=z9hG4bKPjOM1tLyN4eADqKTxYzlBwJgsHAm7F9uU0
        Max-Forwards: 70
        From: <sip:100@192.168.6.176>;tag=vUf7YbHop7dffRHuiMKB9oKuhxeJ0UGs
        To: <sip:100@192.168.6.176>
        Call-ID: BDFu9k3K6LplA8vS6aicb3gWFCgygSVj
        CSeq: 7722 REGISTER
        User-Agent: CSipSimple_WT19i-15/r2457
        Contact: <sip:100@192.168.6.12:47705;ob>
        Expires: 900
        Allow: PRACK, INVITE, ACK, BYE, CANCEL, UPDATE, INFO, SUBSCRIBE, NOTIFY, REFER, MESSAGE, OPTIONS
        Content-Length:  0
```

Obrázek 2.3: Dekódované pakety registrace telefonu

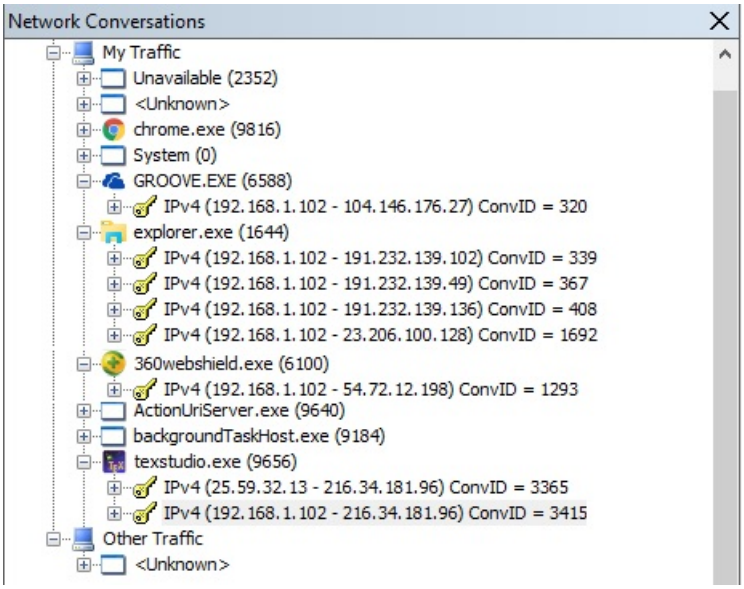
2.2 Microsoft Network Monitor 3.4

Microsoft Network monitor 3.4 je paketový analyzátor doporučený společností Microsoft. Microsoft Network Monitor je zdarma ke stažení na stránkách Microsoftu v sekci ke stažení, případně přímý odkaz v seznamu literatury [7]. Jelikož MNM dokáže zachytávat data z různých karet současně a zobrazovat zachycená data paralelně v oddělených oknech, je třeba si při každém spuštění vytvořit relaci zachytávání tlačítkem "New Capture". Po vytvoření relací 1 - x je třeba pro každou relaci definovat zdroj dat. Pro toto nastavení hledáme tlačítko "Capture Settings". V horní části lze načíst přednastavené filtry pro často hledané služby. Spodní část okna obsahuje seznam síťových karet, kde si jednoduše vybereme odkud chceme data zachytávat (viz Obrázek 2.4.). Po nastavení zdroje dat klikneme na tlačítko start a začnou se objevovat zachycené pakety.



Obrázek 2.4: Okno nastavení zachytávání

Užitečnou vlastností programu Microsoft Network Monitor (MNM) je přehled původu dat, tj. poskytuje možnost identifikace aplikací, z nichž data pocházejí. To nám umožňuje analyzovat pouze data odeslaná aplikací, u níž máme podezření na škodlivý provoz (viz Obrázek 2.5.). Tato možnost je ale omezená na komunikaci počítače, kde je analyzátor nainstalován.



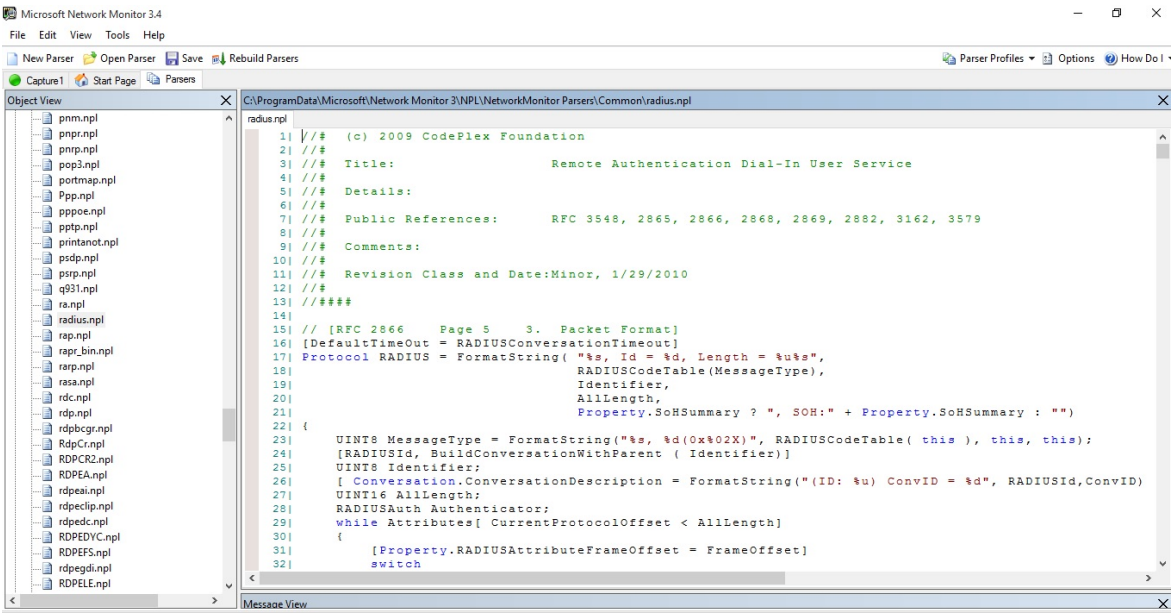
Obrázek 2.5: Aplikace generující provoz do síťe

Okno pro výběr rámců má několik přednastavených konfigurací, měníme je pomocí tlačítka ”Columns”. Každá konfigurace je uzpůsobená pro uživatelovy nejpotřebnější analýzy (”TCP troubleshoot, HTTP troubleshoot”). Součástí každé přednastavené konfigurace je sloupec ”Description”jež nám zobrazuje ve zkratce výpis hlavních vlastností každého rámce. Ten se mění v závislosti na analyzovaném protokolu (viz Obrázek 2.6.). Okno si také můžeme přizpůsobit dle svých preferencí potřeb. Mezi standardně používané sloupce, jež jsou zobrazovány u všech analyzátorů (zdrojová a cílová adresa, číslo paketu, protokol atd.), lze u MNM přidat sloupec dle vlastního výběru. Sloupec dle vlastního výběru můžeme vybrat pomocí volby Columns - Choose Columns.

MNM poskytuje výběr stovek parserů, jež nám z rámce vyberou potřebnou část. Uživateli je umožněn náhled a modifikace kódu parseru a v případě chyby je možno na stránkách vývojářů stáhnout kompletní archiv se všemi parsery. Zdrojový kód parserů je komentován a u většiny lze nalézt odkazy na jednotlivé RFC popisující formát paketu daného standardu (viz Obrázek 2.7.). K oknu s parsery se dostaneme přes záložku ”Parsers”v hlavním okně analyzátoru.

Frame Number	Source	Destination	Protocol Name	Description
42553	[E839DF BDD388]	[*BROADCAST]	WiFi	WiFi:[ManagementBeacon] ....., RSSI = -63 dBm, Rate = 1.0 Mbps, SSID = Middle-Earth, Channel = 6
42555	[E839DF BDD388]	[*BROADCAST]	WiFi	WiFi:[ManagementBeacon] ....., RSSI = -63 dBm, Rate = 1.0 Mbps, SSID = Middle-Earth, Channel = 6
42557	[E839DF BDD388]	[*BROADCAST]	WiFi	WiFi:[ManagementBeacon] ....., RSSI = -61 dBm, Rate = 1.0 Mbps, SSID = Middle-Earth, Channel = 6
42558	[ACA213 C0C...	[*BROADCAST]	WiFi	WiFi:[ManagementBeacon] ....., RSSI = -93 dBm, Rate = 1.0 Mbps, SSID = PotvoraK, Channel = 10
42559	[E839DF BDD388]	[*BROADCAST]	WiFi	WiFi:[ManagementBeacon] ....., RSSI = -63 dBm, Rate = 1.0 Mbps, SSID = Middle-Earth, Channel = 6
42560	[E839DF BDD388]	[*BROADCAST]	WiFi	WiFi:[ManagementBeacon] ....., RSSI = -62 dBm, Rate = 1.0 Mbps, SSID = Middle-Earth, Channel = 6
42561	[E839DF BDD388]	[*BROADCAST]	WiFi	WiFi:[ManagementBeacon] ....., RSSI = -64 dBm, Rate = 1.0 Mbps, SSID = Middle-Earth, Channel = 6
42565	[E839DF BDD388]	[*BROADCAST]	WiFi	WiFi:[ManagementBeacon] ....., RSSI = -62 dBm, Rate = 1.0 Mbps, SSID = Middle-Earth, Channel = 6
42566	[E839DF BDD388]	[*BROADCAST]	WiFi	WiFi:[ManagementBeacon] ....., RSSI = -62 dBm, Rate = 1.0 Mbps, SSID = Middle-Earth, Channel = 6
42568	[E839DF BDD388]	[*BROADCAST]	WiFi	WiFi:[ManagementBeacon] ....., RSSI = -63 dBm, Rate = 1.0 Mbps, SSID = Middle-Earth, Channel = 6
42569	[ACA213 C0C...	[*BROADCAST]	WiFi	WiFi:[ManagementBeacon] ....., RSSI = -93 dBm, Rate = 1.0 Mbps, SSID = PotvoraK, Channel = 10
42570	[E839DF BDD388]	[*BROADCAST]	WiFi	WiFi:[ManagementBeacon] ....., RSSI = -63 dBm, Rate = 1.0 Mbps, SSID = Middle-Earth, Channel = 6
42571	[E839DF BDD388]	[*BROADCAST]	WiFi	WiFi:[ManagementBeacon] ....., RSSI = -63 dBm, Rate = 1.0 Mbps, SSID = Middle-Earth, Channel = 6
42572	[E839DF BDD388]	[*BROADCAST]	WiFi	WiFi:[ManagementBeacon] ....., RSSI = -63 dBm, Rate = 1.0 Mbps, SSID = Middle-Earth, Channel = 6
42576	[E839DF BDD388]	[*BROADCAST]	WiFi	WiFi:[ManagementBeacon] ....., RSSI = -62 dBm, Rate = 1.0 Mbps, SSID = Middle-Earth, Channel = 6
42577	[E839DF BDD388]	[*BROADCAST]	WiFi	WiFi:[ManagementBeacon] ....., RSSI = -64 dBm, Rate = 1.0 Mbps, SSID = Middle-Earth, Channel = 6

Obrázek 2.6: Okno rámců protokolu 802.11

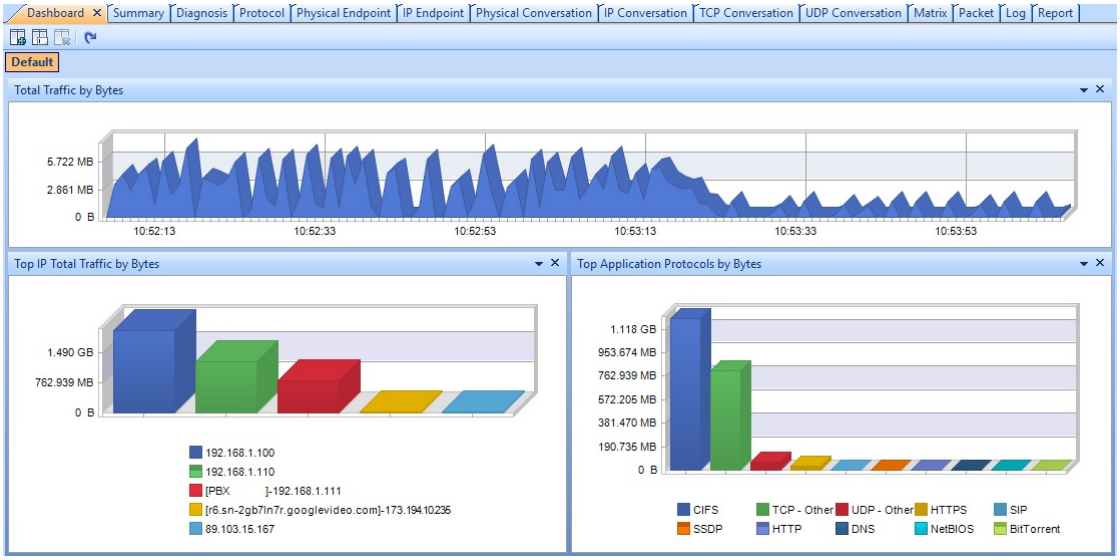


Obrázek 2.7: Parser protokolu RADIUS

2.3 Colasoft Capsa

Je převážně podnikový analyzátor. Společnost Colasoft poskytuje analyzátor i ve free verzi, který můžete stáhnout pomocí odkazu [1]. Verze zdarma má sice dostupné veškeré hlavní funkce analyzátoru, ale má omezenou velikost sítě na 10 zařízení a umožňuje v bufferu uložit k další analýze pouze 8 MB dat. Veškeré pakety nad rámec tohoto omezení jsou zahazovány a pro vlastní hlubší analýzu nedostupné. Tato verze nám ale postačí k anylýze domácí sítě a k plné demonstraci vlastností tohoto analyzátoru. Pokud chceme analyzátor vyzkoušet ve větší síti, je možné po registraci stáhnout trial verzi Enterprice verzi, což nám umožní užívat zablokovaných vlastností a vyšší paměti po dobu patnácti dnů. Registraci pro stažení trial licence můžete provést pomocí odkazu [2].

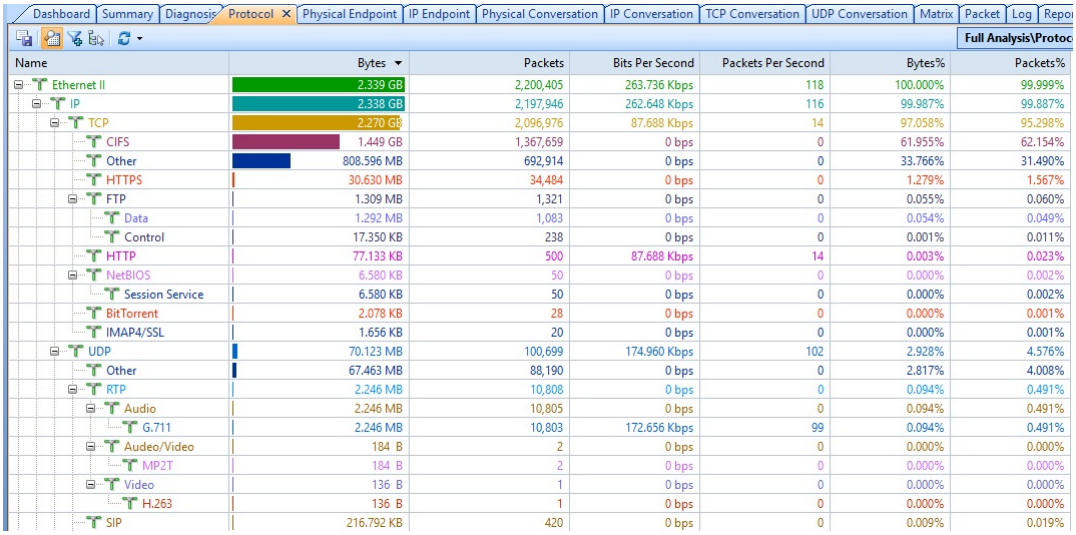
Primární funkcí tohoto analyzátoru je poskytnutí globálního přehledu o provozu v síti. Hlavní okno analyzátoru obsahuje záložky s aktuálními daty analýzy v tabulkách a grafech. První záložka - dashboards - nám poskytuje prostor pro grafy informací, které potřebujeme sledovat. Můžeme si okno přizpůsobit jak funkčně, tak vizuálně dle svých potřeb a představ. Příklad můžeme vidět na obrázku 2.8.



Obrázek 2.8: Graf aktuálního vytížení, pět nejvíce komunikujících adres, graf nejvíce používaných protokolů

Další záložka - summary - obsahuje souhrnné tabulkové zpracování analyzovaných informací. Tabulky obsahují např.: počet bezpečnostních varování, počet diagnostických zpráv, množství broadcast provozu, multicast provozu, množství paketů určité velikosti, počet jednotlivých typů adres, počet HTTP či DNS dotazů, atd. Další záložka - diagnostics - ulehčuje hledání paketů s problematickým chováním na aplikační nebo transportní vrstvě(neexistující DNS záznam, pomalá TCP odpověď). V seznamu informativních hlášení vybereme problém, který chceme řešit. Poté se v jedotlivých podoknech můžeme dozvědět MAC, IP adresy, jež disponují tímto problémem, případně můžeme dvojkliknutím zobrazit rovnou chybný paket. Záložka protocol poskytuje přehled množ-

ství dat a paketů jenotlivých protokolů na všech vrstvách ISO/OSI modelu, ukázkový výpis můžete vidět na obrázku 2.9.



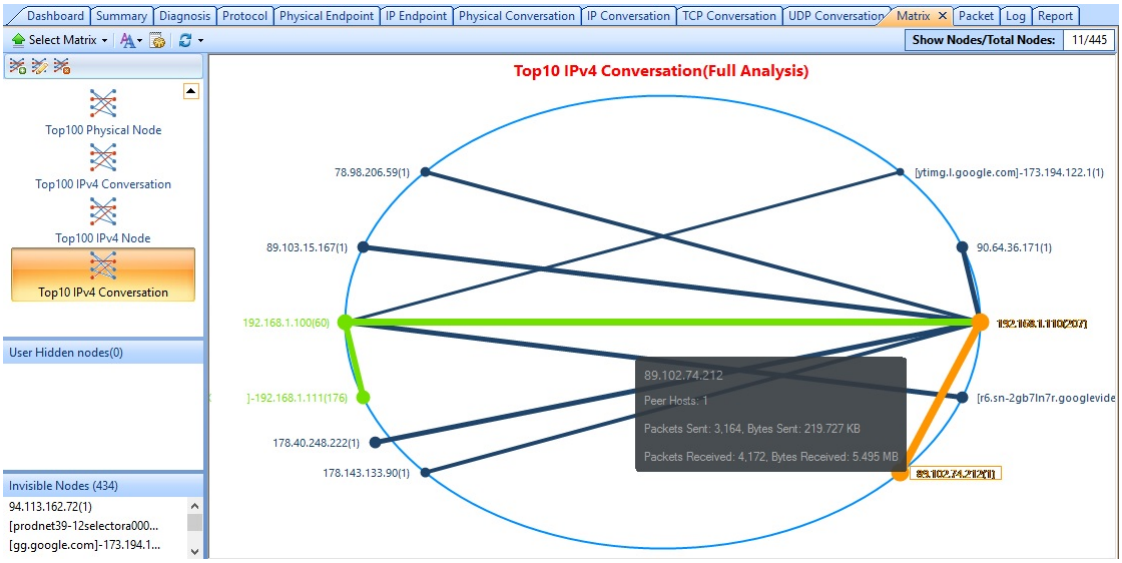
Dashboard | Summary | Diagnosis | Protocol | Physical Endpoint | IP Endpoint | Physical Conversation | IP Conversation | TCP Conversation | UDP Conversation | Matrix | Packet | Log | Repo

Full Analysis\Protoc

Name	Bytes	Packets	Bits Per Second	Packets Per Second	Bytes%	Packets%
Ethernet II	2.339 GB	2,200,405	263.736 Kbps	118	100.000%	99.999%
IP	2.338 GB	2,197,946	262.648 Kbps	116	99.987%	99.887%
TCP	2.270 GB	2,096,976	87.688 Kbps	14	97.058%	95.298%
CIFS	1.449 GB	1,367,659	0 bps	0	61.955%	62.154%
Other	808.596 MB	692,914	0 bps	0	33.766%	31.490%
HTTPS	30.630 MB	34,484	0 bps	0	1.279%	1.567%
FTP	1.309 MB	1,321	0 bps	0	0.055%	0.060%
Data	1.292 MB	1,083	0 bps	0	0.054%	0.049%
Control	17.350 KB	238	0 bps	0	0.001%	0.011%
HTTP	77.133 KB	500	87.688 Kbps	14	0.003%	0.023%
NetBIOS	6.580 KB	50	0 bps	0	0.000%	0.002%
Session Service	6.580 KB	50	0 bps	0	0.000%	0.002%
BitTorrent	2.078 KB	28	0 bps	0	0.000%	0.001%
IMAP4/SSL	1.656 KB	20	0 bps	0	0.000%	0.001%
UDP	70.123 MB	100,699	174.960 Kbps	102	2.928%	4.576%
Other	67.463 MB	88,190	0 bps	0	2.817%	4.008%
RTP	2.246 MB	10,808	0 bps	0	0.094%	0.491%
Audio	2.246 MB	10,805	0 bps	0	0.094%	0.491%
G.711	2.246 MB	10,803	172.656 Kbps	99	0.094%	0.491%
Audeo/Video	184 B	2	0 bps	0	0.000%	0.000%
MP2T	184 B	2	0 bps	0	0.000%	0.000%
Video	136 B	1	0 bps	0	0.000%	0.000%
H.263	136 B	1	0 bps	0	0.000%	0.000%
SIP	216.792 KB	420	0 bps	0	0.009%	0.019%

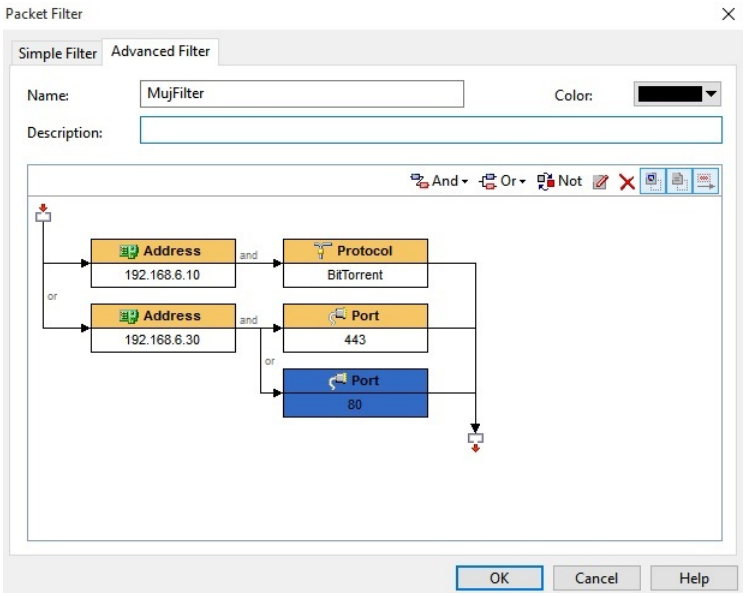
Obrázek 2.9: Tabulka výskytu jednotlivých protokolů

Záložka physical adress poskytuje přehled IP adres, jež jsou dostupné na určitých MAC adresách. Oproti tomu v záložce IP endpoints se dozvíme, kolik Byte dat bylo vyměněno mezi kterými IP adresami. Dále například informace o zemi původu jednotlivé IP adresy. Lze se tedy dozvědět zemi, kde nejvíce proudí data z naší sítě. Další záložky - IP, TCP, UDP conversations - umožňují jednoduše vyhledat pakety jednotlivých datových výměn. V záložce matrix (viz Obrázek 2.10) máme formou pavučiny graficky znázorněny datové výměny mezi jednotlivými adresami. Záložka packet je klasické hlavní okno většiny analyzátorů a najdeme v něm výčet veškerých zachycených paketů s parametry, jež nám umožní jejich lepší identifikaci (zdrojová adresa, cílová adresa, protokol). Předposlední záložka - log - obsahuje několik přednastavených logů služeb v síti, kde každý poskytuje podrobné informace o jednotlivých službách. Např. datum a čas FTP přenosu s infomacemi o účtu clienta, velikosti souboru, doby přenosu, počtu paketů přenosu atd. Poslední záložka - report - je typickou pro podnikový analyzátor a poskytuje uživateli možnost vyexportovat shrnutí veškerých statistik o síťovém provozu ve formátu .pdf.



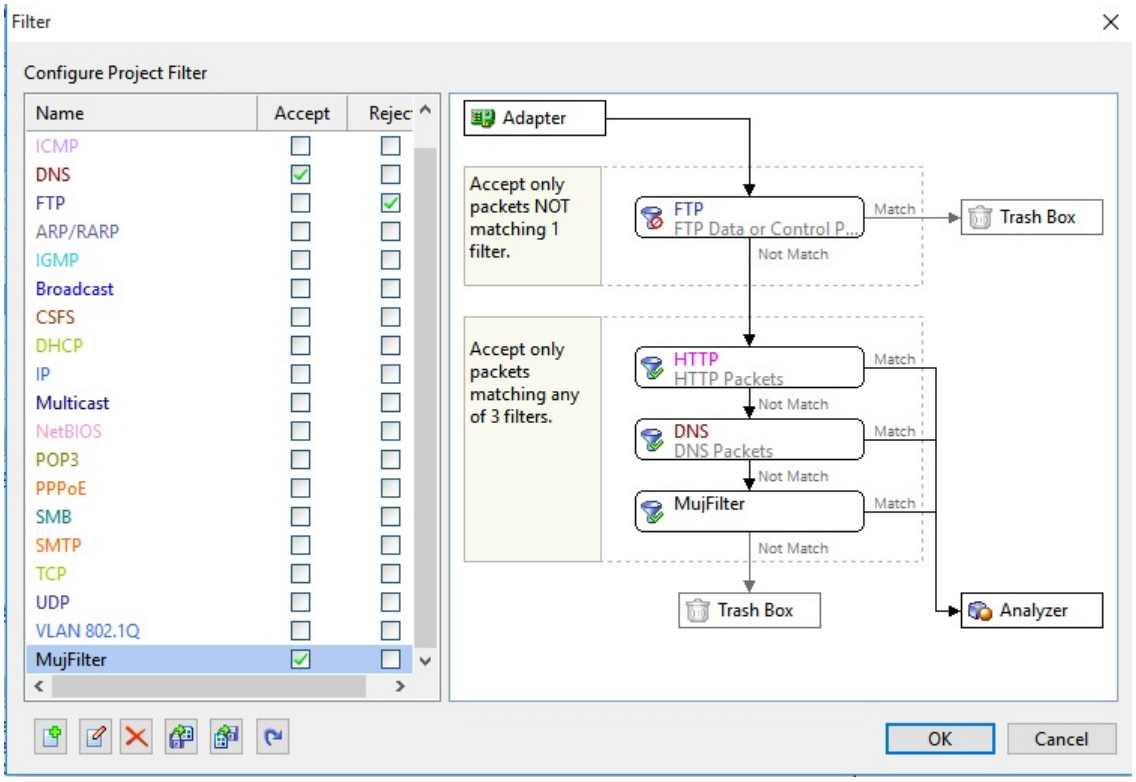
Obrázek 2.10: Pavučina 10 nejvíce komunikujících zařízení

Analyzátor do verze 8 neposkytuje filtrační pravidla pro vyhledávání v paketech, ale pouze pravidla pro filtrování paketů, jenž mají být uchovány k analýze, což komplikuje vyhledání specifického paketu v již zachycených paketech. V první fázi filtru můžeme zvolit jednoduchý filtr na bázi MAC/IP/Portu, nebo můžeme zvolit pokročilý filter a poskládat si pomocí grafického rozhraní sofistikovanější filtr složený z mnoha základních filtrů a logických operátorů, které známe z tvorby filtrů u jiných analyzátorů (viz Obrázek 2.11.).



Obrázek 2.11: Pokročilý filr pro torrent a webové stránky 1. fáze

Po potvrzení přejdeme k druhé fázi filtrace, kde volíme zda naše filtry mají data pro anylýzu vybírat či data, která projdou filtrem, zahazovat. Aplikace filtru i jejich pořadí je graficky znázorněno, jak můžeme vidět na obrázku 2.12



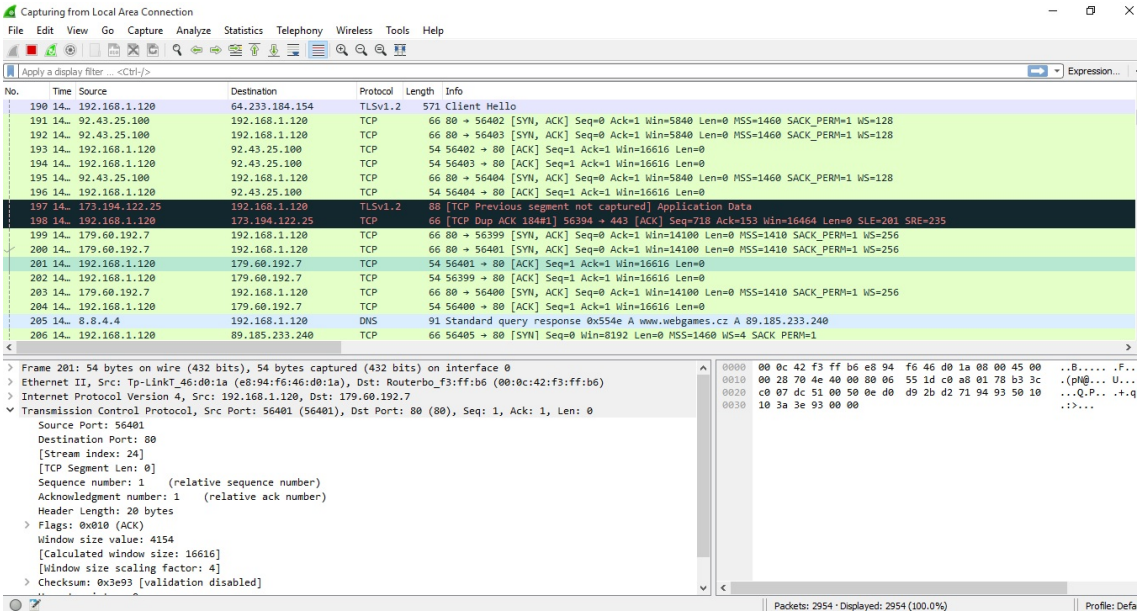
Obrázek 2.12: Pokročilý filr pro torrent a webové stránky 2. fáze

2.4 Wireshark

Wireshark je světově nejpopulárnější multiplatformní freewareový paketový analyzátor. Na Linuxu lze nainstalovat příkazem ”sudo apt-get install wireshark”. Pro uživatele Windows a OSX je dostupný ke stažení pomocí odkazu [3]. Na stránkách [15] je ze strany vývojářů poskytnut podrobný manuál jak s programem pracovat.

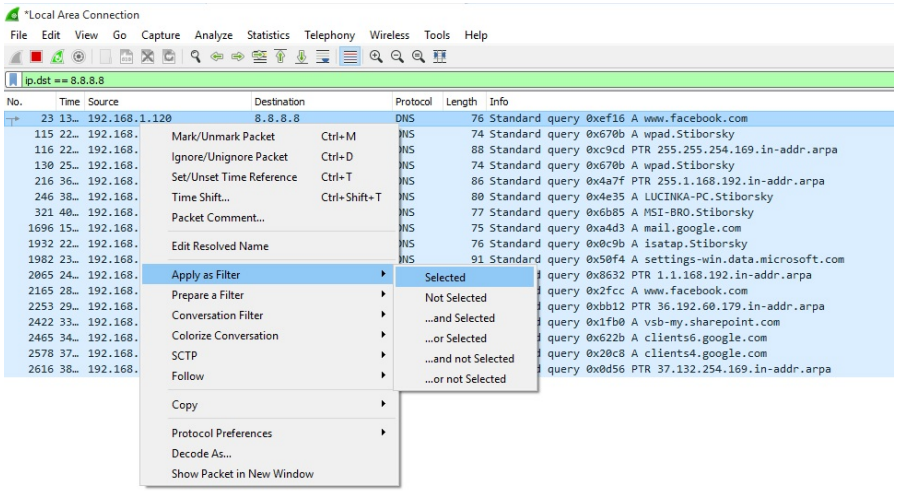
Po spuštění Wiresharku je třeba definovat síťovou kartu pro zachytávání dat. Můžeme použít tlačítko interface list pro základní informace o adresách a množství provozu na jednotlivých rozhraních. Případně rychlou volbou označením karty v úvodním okně programu. Po výběru spustíme zachytávání tlačítkem s ikonou zelené hřbetní ploutve žraloka.

Po výběru jedné nebo více síťových karet se v hlavním okně zobrazují aktuálně zachycené pakety. Jednotlivé protokoly jsou barevně odlišeny, což uživateli poskytuje rychlejší přehled o aktuálním provozu v síti. Při označení paketu lze v poli pod hlavním oknem rozkliknout a prohlížet obsah paketů po jednotlivých vrstvách ISO/OSI modelu. Vedlejší pole obsahuje nedekódovaná data v hexadecimálním vyjádření (viz Obrazek 2.13.).



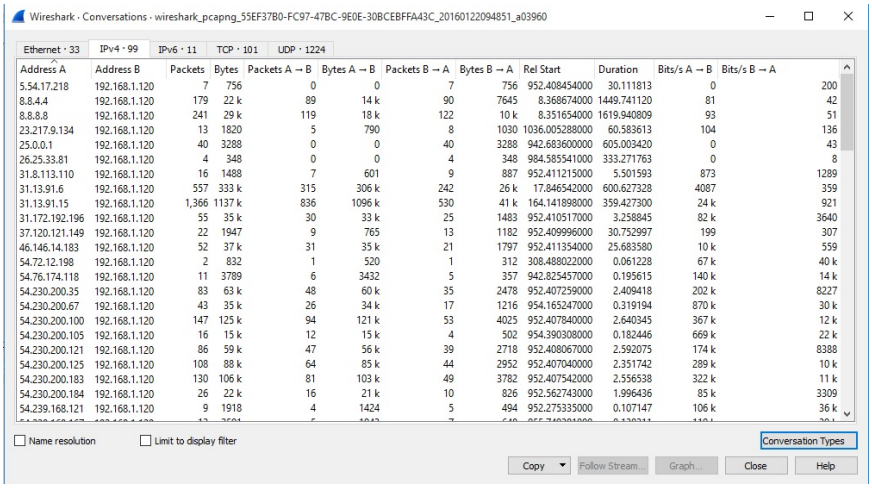
Obrázek 2.13: Hlavní okno analyzátoru

Pro výběr určitých paketů používáme filtrační pravidla. Tvorbu filtračních pravidel nám ulehčí možnost vytváření filtru pomocí pravého tlačítka myši na požadovaný protokol či adresu, jak lze vidět na obrázku 2.14.



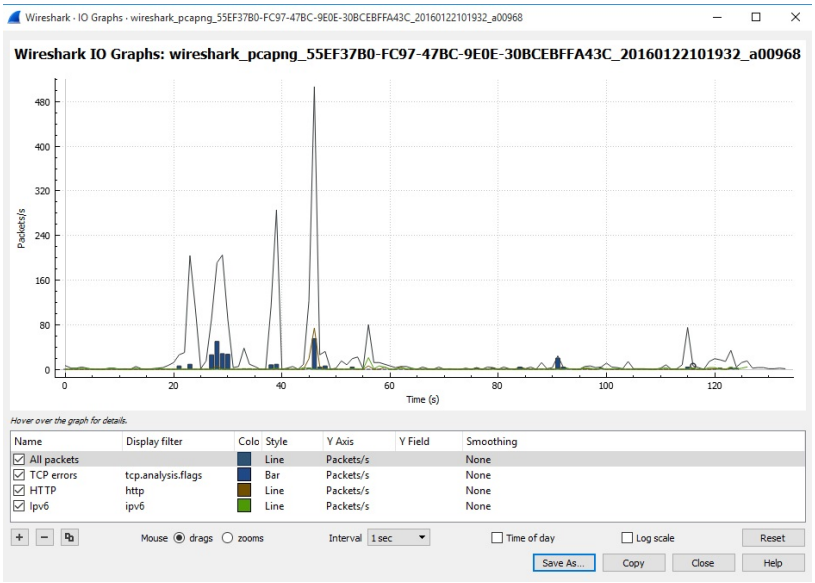
Obrázek 2.14: Vytváření filtračního pravidla pomocí klikací volby

Analyzátor poskytuje několik možností statistického zpracování provozu v síti. Příkladem může být statistika konverzací v síti, která zobrazí množství vyměněných dat mezi zařízeními. Záložkou v okně můžeme volit konverzace jednotlivých MAC adres, IPv4, IPv6, TCP či UDP streamů (viz Obrázek 2.15.).



Obrázek 2.15: Statistika IPv4 konverzací

Další užitečnou funkcí je tvorba grafu dle vlastního filtru. Nevýhodou grafových filtrů je nezobrazení nápovědy možných parametrů při psaní potřebného filtru, tudíž se při psaní složitějšího filtru neobejdeme bez manuálu k programu. Ukázkový graf vidíme na obrázku 2.16.



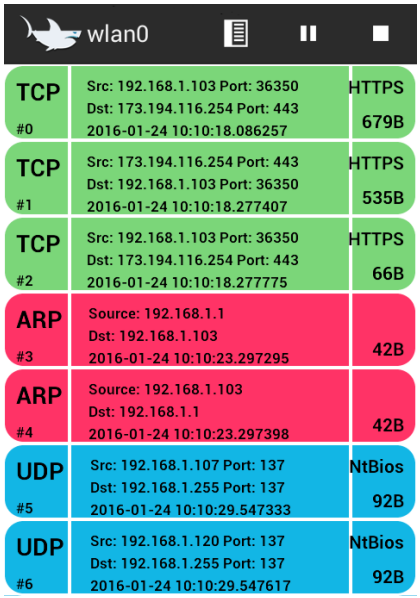
Obrázek 2.16: Ukázkový graf událostí v síti

Graf toku (flow graph) je nástroj, jež zobrazuje chronologickou posloupnost jednotlivých paketů se základním popisem důležitých aspektů, což nám ulehčuje orientaci v grafu. Využití tohoto nástroje je složité, proto se k němu vrátíme v kapitole se speciálními vlastnostmi analyzátorů.

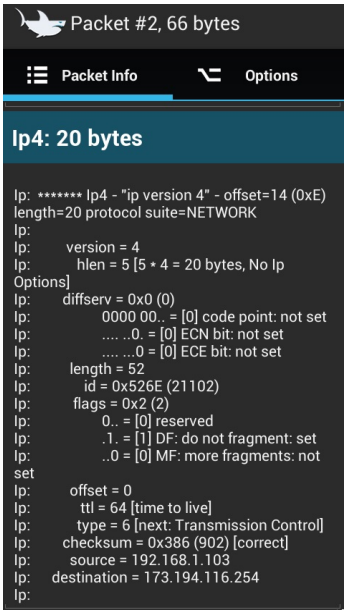
V záložce statistics nalezneme mnoho dalších funkcí jako je například překlad adres, který obsahuje nejen zachycené DNS záznamy v síti, ale také přiřazení fyzických adres k jednotlivým výrobcům. Dále poslouží protokolová hiearchie v případě analýzy zastoupení jednotlivých protokolů v síťovém provozu. Statistické funkce také poskytují analýzu odezvy častých služeb v síti jako RADIUS, DIAMETER, SMB, LDAP atd., ty nám mohou být užitečné při řešení problému s výkonem sítě.

2.5 BitShark

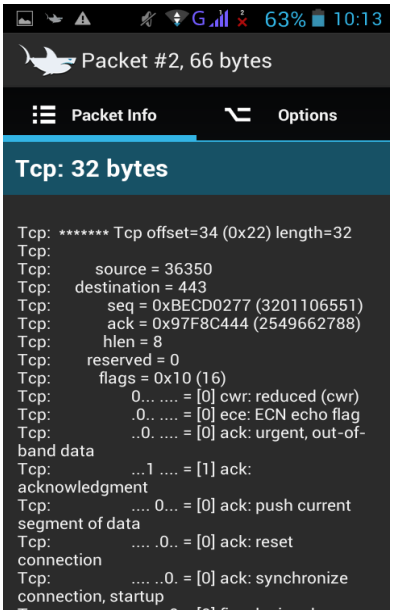
BitShark je obdoba Wiresharku pro Android 2.3.3. a výše. Aplikace je dostupná na Google play za 59 Kč. Přímý odkaz k instalaci naleznete zde: [4] Pro její užívání musí mít uživatel práva administrátora (root), což může být u některých mobilů problém, jelikož uživatel v mnoha případech tímto ztrácí záruku na dané zařízení. Při prvotním nastavení je potřeba vybrat rozhraní, z kterého chceme pakety zachytávat, případně použít zachytávací filtr. Filtr na rozhraní se píše v libcap syntaxi, což je syntaxe filtrů pro textový analyzátor TCPDUMP. Pokud chceme zachytávat všechna data, pouze vybereme rozhraní a spustíme zachytávání. Protokoly aktuálně zachycených paketů jsou barevně odlišeny v barvách na které jsme již zvyklí z klasického Wiresharku (viz Obrázek 2.17.).



Obrázek 2.17: Aktuálně zachycené pakety



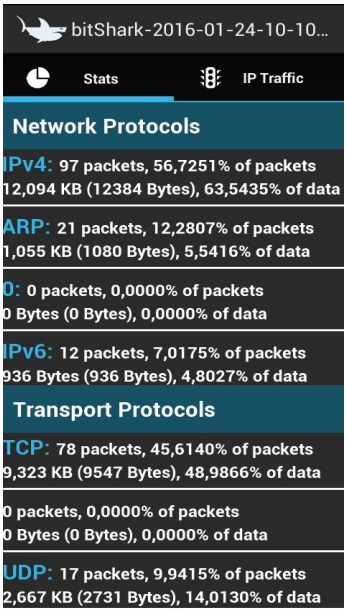
Obrázek 2.18: IPv4 hlavička paketu



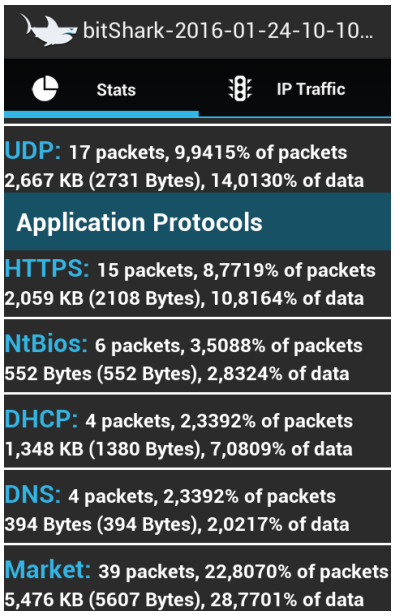
Obrázek 2.19: Hlavička transportní vrstvy

Po vybrání potřebného paketu můžeme postupně prohlížet všechny vrstvy paketu. Na obrázcích 2.18, 2.19, lze vidět obsah hlaviček příkladového paketu.

Po ukončení zachytávání lze provést celkovou analýzu obsahu paketů. Výsledky analýzy zobrazují např. množsví byte přenesených v paketech, poměr protokolů na všech vrstvách v zachycených paketech, množství dat vyměněných v rámci jednotlivých TCP /UDP streamech či dokódované obrázky zachycené z HTTP paketů. Příkladovou statistiku krátkého zachytávání naleznete na obrázcích 2.20 a 2.21. Veškeré zpracované statistiky se dají exportovat do .pfd formátu.

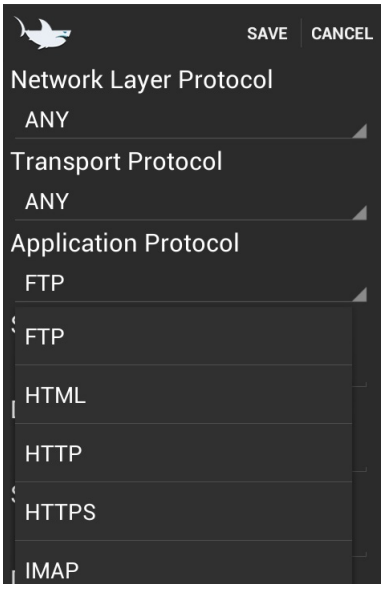


Obrázek 2.20: Statistika protokolů transportní a síťové vrstvy



Obrázek 2.21: Statistika protokolů na aplikační vrstvě

Po ukončení zachytávání může uživatel využít vytváření filtrů pomocí klikací předvolby, jež při rozkliknutí zobrazí nápovědu protokolů, které můžeme na dané vrstvě filtrovat (viz Obrázek 2.22.).



Obrázek 2.22: Vytoření filtru pomocí klikací volby

Mezi další užitečné vlastnosti analyzátoru bitshark je možnost exportovat jednotlivé pakety v PCAP formátu pro analýzu v jiném programu, či využití v generátorech provozu. Aplikace umí zpětně načíst a analyzovat pakety uložené v PCAP formátu z jiných analyzátorů.

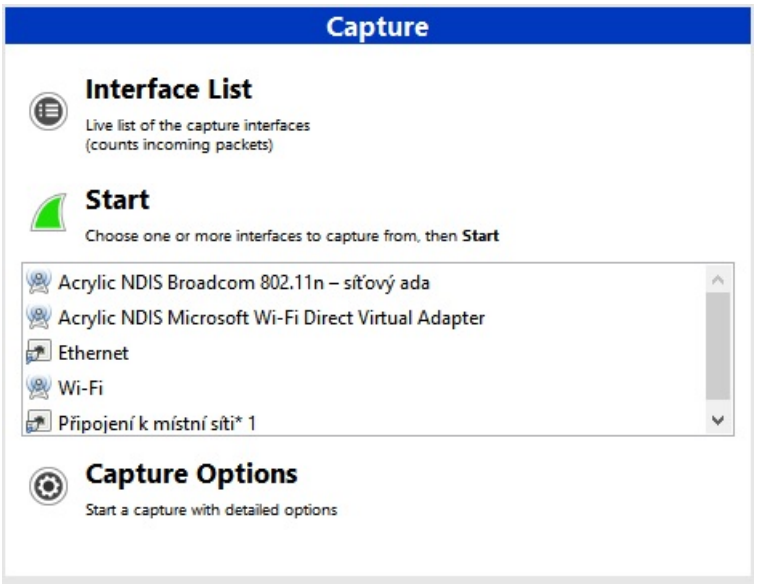
3 Speciální funkce analyzátorů

3.1 Wireshark

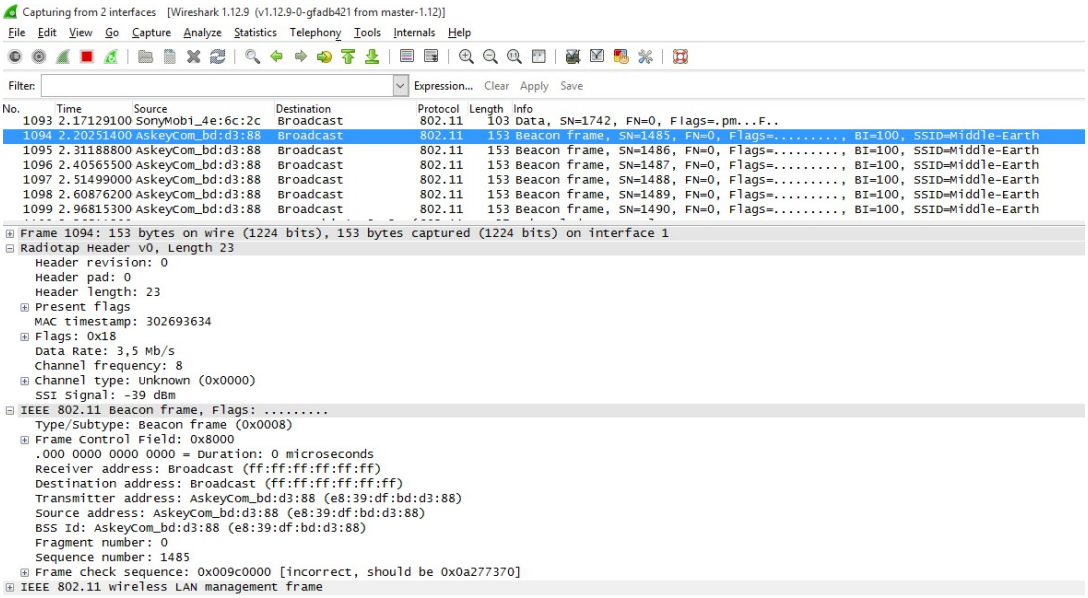
3.1.1 Analýza 802.11 rámců

Jeden z nedostatků Wiresharku je, že veškerý provoz zachycený na síťových kartách, jak ethernetových tak wifi, analyzátor klasifikuje jako ethernet (802.3). Tudíž nemůžeme analyzovat informace ukryté v rámcích 802.11. Pro tento účel je třeba mít speciální USB síťovou kartu Riverbed AirPcap, jejíž varianta pro standrardy b,g,n se v osobní edici prodává za 698$. [9] Pro převážnou část uživatelů je tato částka příliš vysoká a tudíž komunita našla náhradu. Náhradní alternativou tohoto hardwaru může být program Acrylic WiFi Professional, jehož součástí je NDIS driver obsahující AirPcap emulátor. K našemu účelu postačí stažení trial licence, jelikož ovladače můžeme dále používat i po vypršení této licence. Acrylic WiFi Professional naleznete pomocí odkazu [13].

Při instalaci je třeba zvolit rozšířenou instalaci a přidat k základnímu programu i balíčky pro hardwarovou emulaci síťové karty. Instalace upozorňuje, že emulace je možná pouze pro podporované karty a před instalací je třeba ověřit, zda-li je naše karta podporována. Aktuální seznam podporovaných síťových karet nalezneme zde: [12]. Po instalaci programu je třeba spouštět Wireshark jako zprávce, aby načetl knihovny ovladače. K analýze můžeme vybrat interní síťovou kartu pro zachytávání dat nebo virtuální kartu viz Obrázek 3.1. Virtuální síťová karta nám v promiskuitním režimu zachytí rámce z frekvenčního pásma naší síťové karty viz Obrázek 3.2. Vývojáři tohoto software upozorňují, že ne všechny ovladače karet jsou vhodné pro zachytávání wifi provozu. Některé karty mají problém s kompatibilitou zachytávání rámců v 40/80 MHz kanálech, a proto jako dobrého zástupce harwarové karty spolu s ovladačem NDIS vývojáři doporučují USB kartu Netgear A6200, jejíž cena se pohybuje okolo 13$.



Obrázek 3.1: Nové NDIS virtuální karty



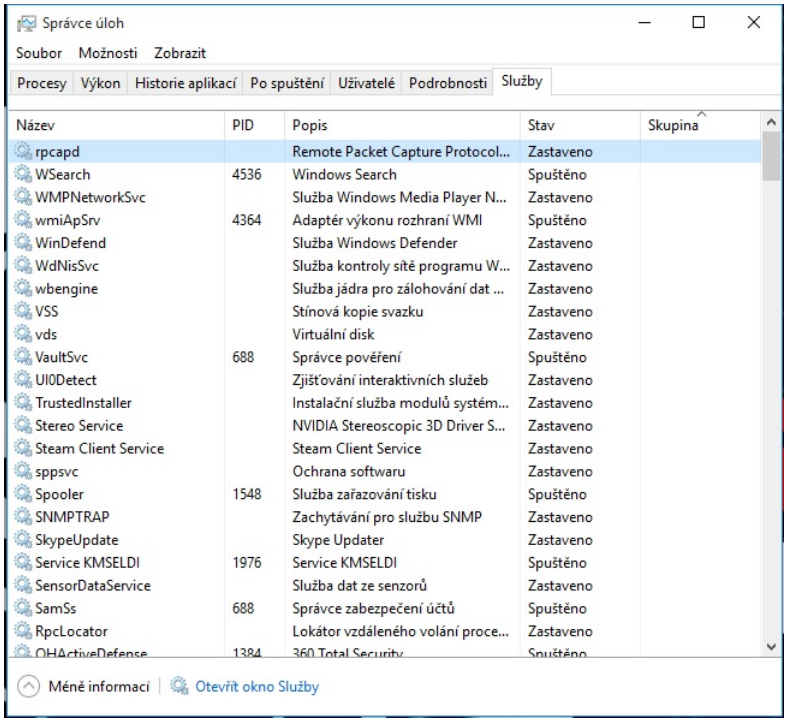
Obrázek 3.2: Zachytávané wifi rámce

3.1.2 Zachytávání paketů na vzdáleném rozhraní

Pokud potřebujeme zachytávat data na vzdáleném zařízení, oceníme vlastnost Wiresharku - připojení na vzdálené rozhraní pomocí RPCAPD (Remote Packet Capcure Protocol). RPCAPD je pro systém Windows součástí ovladače WinPcap, s jehož pomocí přepíná Wireshark rozhraní do promiskuitního režimu. Pokud na zařízení nepotřebu-

jeme Wireshark ale jde nám pouze o funkci vzdáleného zachytávání, můžeme ovladač stáhnout a nainstalovat samostatně z odkazu [10].

Poté službu nalezneme ve správci úloh a spustíme pomocí pravého tlačítka myši + spustit, viz Obrázek 3.3.

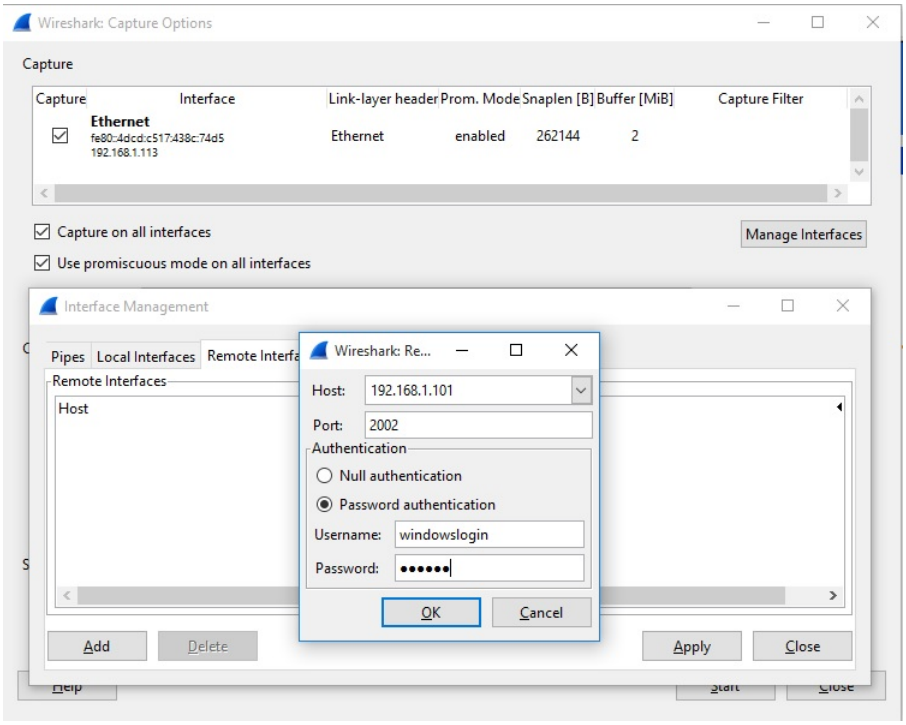


Obrázek 3.3: Službu RPCAPD je třeba ručně vyhledat a spustit

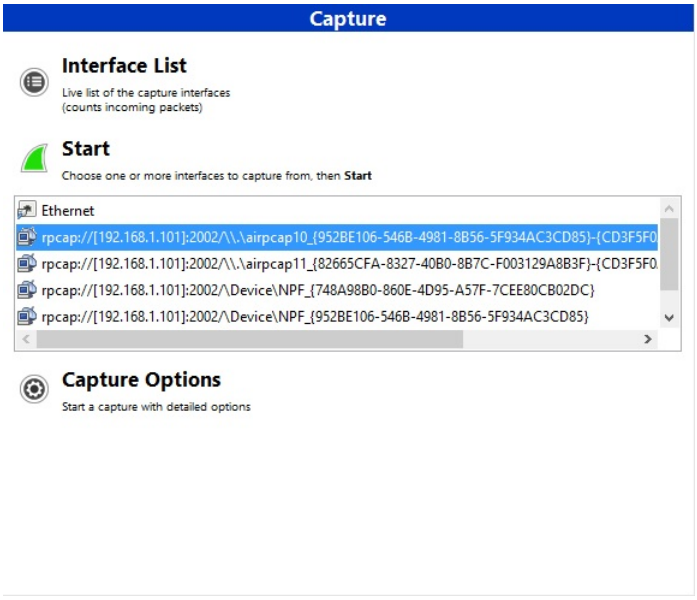
Po spuštění RPCAPD protokolu na zařízení, které nám bude sloužit jako vzdálený paketový zachytávač, přejdeme k nastavení Wireskarku na zařízení, které bude plnit funkci paketové analýzy. K nastavení se dostaneme pomocí cesty : Capture options - Manage Interfaces - Remote Interfaces - Add. Celé nastavení je shrnuto na obrázku 3.4. RPCAPD protokol používá ve výchozím stavu port 2002 a je třeba se ujistit, že máme na daný port ve firewallu povolen přístup. Případně jednoduše windows firewall vypneme. Ostatní parametry nastavení z obrázku 3.4 jsou inviduální a jsou zde uvedeny pouze demonstrativní hodnoty.

Po úspěšném přihlášení a připojení vzdáleného rozhraní se k rozhraním lokálního počítače přidají i všechna rozhraní počítače vzdáleného viz Obrázek 3.5.

Protokol RPCAPD je momentálně experimentální protokol kompatibilní pouze s Windows zařízeními. Vzdálené zachytávání z Linux zařízení je momentálně možné pouze pomocí programu TCPDUMP, jehož výpis posíláme přes SSH tunel do FIFO adresáře. Wireshark následně data z adresáře čte a analyzuje. Postup je následující: V adresáři /tmp vytvoříme adresář pro naši pipe pomocí příkazu: ”sudo mkdir pipes”Následně do adresáře vytvoříme FIFO pipe: mkfifo /tmp/pipes/RemoteData



Obrázek 3.4: Demonstrativní nastavení vzdáleného rozhraní



Obrázek 3.5: Lokální rozhraní spolu se všemi vzdáleně připojenými rozhraními

Před spojením je třeba mít na vzáleném zařízení nainstalovaný TCPDUMP, viz předchozí kapitola. Po instalaci programu TCPDUMP na vzdálené rozhraní lze připojit vzdá-

lené zařízení k našemu adresáři příkazem: ssh root@adresa ”tcpdump -s 0 -U -n -w - -i eth0 not port 22» /tmp/pipes/RemoteData

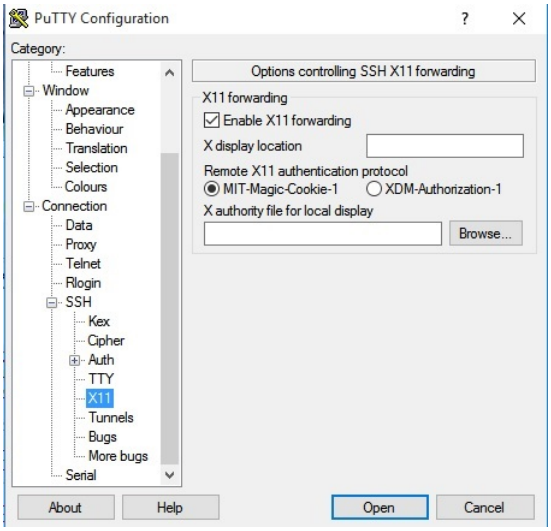
Parametr -s 0 je potřebný k zachycení celých paketů. Parametr -U zapisuje paket do pipe okamžitě po zachycení. Parametrem -n nechceme překládat adresy na doménová jména před přenosem (může provést samotný wireshark). Parametrem -w - zapisujeme výstup jako standardní výstup. Parametrem -i eth0 definujeme vzdálené rozhraní. Parametr ”not port 22”je zde z důvodu přenosu dat pomocí ssh na portu 22, jinak by se data posílala podruhé v zašifrované podobě. Parametrem » /tmp/pipes/RemoteDevice”přesměrujeme výstup z ssh do našeho adresáře.

Pokud TCPDUMP data zachytává i posílá, je třeba v jiném terminálu spustit wireshark specifickým příkazem: ”wireshark -k -i /tmp/pipes/RemoteDevice”, kde parametr ”-k”přikazuje okamžité spuštění a parametr ”-i /tmp/pipes/RemoteDevice”definuje FIFO adresář jako vstupní rozhraní.

Pro vzdálené zachytávání mezi Windowsem a Linuxem je třeba použít jiných podpůrných nástrojů. V tomto případě nemáme k dispozici FIFO adresář ani protokol RPCAPD, tedy si můžeme pomoci jinak. K propojení těchto zařízení použijeme program X Window System (X11), jež poskytuje základní framework pro grafické rozhraní s interakcí myši a klávesnice. Využívá klient-server model, kde server zpracová dotazy na grafickém rozhraní a zpět posílá uživatelský vstup (klávesnice, myš). Na Linux zařízení je třeba nainstalovat program pomocí ”sudo apt-get install xorg”. Kvalita a vzhled generovaného rozhraní se odvíjí od verze Xming serveru. Máme tedy možnost stáhnout nejnovější originální verzi ze stránek autora programu [5]. Přístup ke stažení instalačního souboru dostaneme za poplatek 10$ na podporu vývoje programu. Další možností je stáhnout některou ze starších Public Domain Licencí, např. 6.9.0.31 z roku 2007, ta je dostupná pomocí odkazu [6]. Propojení probíhá pomocí SSH tunelu. Před každým spojením je třeba upravit nastavení putty a zapnout přenos X11. Úpravu nastavení můžeme vidět na obrázku 3.6.

.

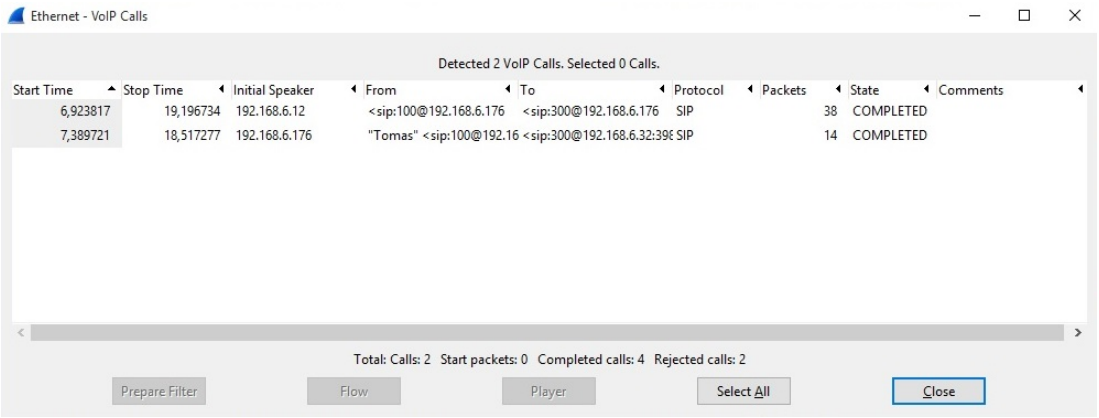
Po připojení na vzdálené zařízení lze spustit wireshark příkazem ”sudo wireshark”a XMing server na počítači vytvoří okno s uživatelským rozhraním wiresharku. Program není omezen pouze na wireshark, lze pustit téměř všechny programy s grafickým rozhraním.



Obrázek 3.6: Spuštění podpory X11

3.1.3 Analýza VOIP a graf toku

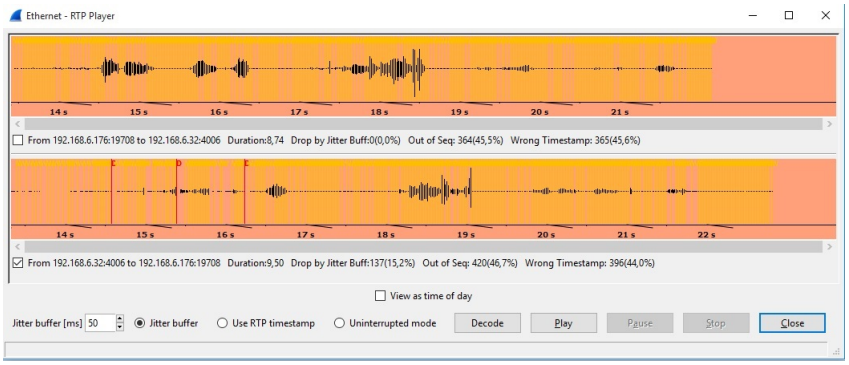
Wireshark má také výborné nástroje pro analýzu VoIP hovorů. Pomocí záložky Telephony - VoIP Calls spustíme automatickou filtraci VoIP spojení pro námi zachycená data. Pro demonstrativní data (viz Obrázek 3.7) vidíme výsledek filtrace pro zachytávání spuštěné na Asterisk serveru. Jedná se o spojení od účastníka 100 s adresou 192.168.6.12 směrem k účastníkovi 300 s adresou 192.168.6.32. Ke spojení byla použita signalizace SIP a hovor proběhl přes ústřednu 192.168.6.176.



Obrázek 3.7: Základní informace o VoIP hovorech

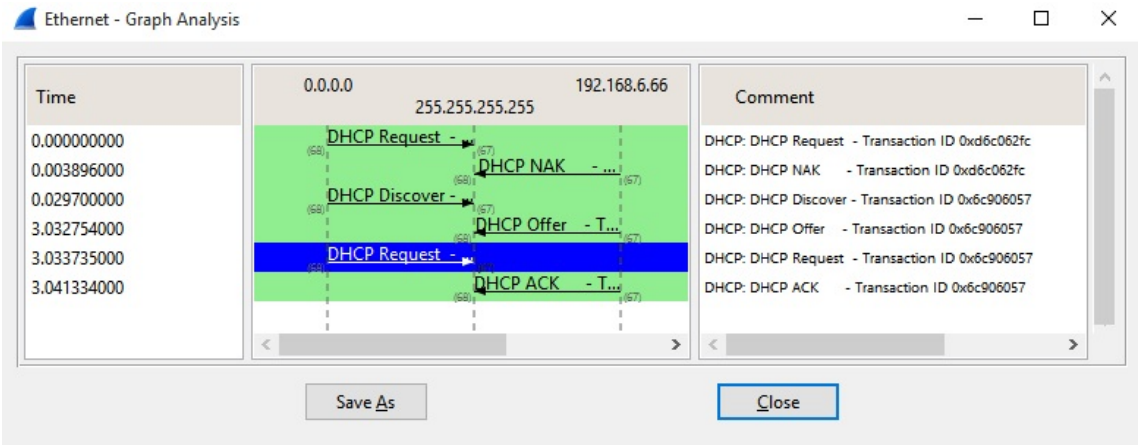
Myší označíme hovor, který nás zajmá, a klikneme na tlačítko player. Po spuštění playeru je třeba daný hovor dekódovat. Klikneme na tlačítko decode a wireshark nám hovory dekóduje a zobrazí diagram vybuzení hlasu (viz Obrázek 3.8).

Nakonec označíme hovor, který chceme přehrát a tlačítkem play přehrajeme.



Obrázek 3.8: Hlasové diagramy hovoru

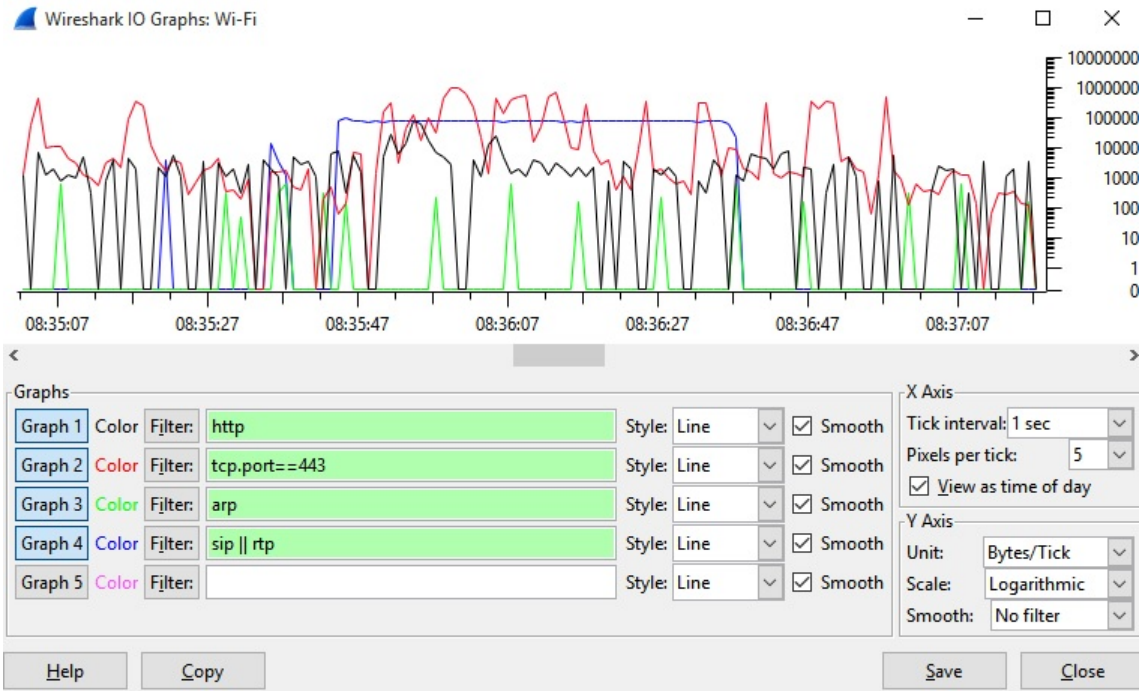
Z okna VoIP Calls můžeme zobrazit graf toku signalizace. Graf toku je chronologicky seřazená posloupnost komunikace, která prošla filtrem. Nyní je filtrační pravidlo VoIP hovor, tudíž zobrazená komunikace se týká našeho spojení. V příloze A je graf komunikace volajícího klienta se serverem. Lze vidět čas jednotlivých zpráv a vyhodnotit tak rychlost odpovědi serveru a dobu vyzvánění. Dále poznáme, kdo hovor ukončil nebo jaký kodek byl použit pro přenos hlasu. Označením specifické zprávy se nám paket označí i v hlavním okně, tudíž je možné provést okamžitou vlastní hloubkovou analýzu paketu a následně vyhledat informaci, kterou potřebujeme vědět. Jak už bylo zmíněno, graf toku není omezen jen na VoIP, ale lze jej využít pro výsledky vlastní filtrace. Příkladově proto použijeme v hlavním okně analyzátoru filter ”udp.port==67 ||udp.port==68”, čímž si filtrujeme komunikaci DHCP. V záložce Statistics klikneme na Flow Graph. V okně nastavení grafu změníme výběr paketů ze všech paketů na zobrazené pakety a potvrdíme. Výsledkem je graf toku, který vidíme na obrázku 3.9.



Obrázek 3.9: Graf toku zpráv DHCP

3.1.4 Využití I/O grafu

Nástroj I/O graf nalezneme v záložce statistics. Jedná se o nástroj, kterým můžeme sledovat množství údálostí v síti. Události vybíráme pomocí klasického filtračního pravidla. Můžeme použít přednastavené, často používané filtry, nebo jednoduše filtrovat protokol, o který máme zájem (viz Obrázek 3.10). Na osu Y můžeme zobrazovat pakety/byte/bity v závislosti na časovém intervalu nastaveném na ose X.



Obrázek 3.10: Počet byte/s protokolů HTTP, HTTPS, ARP, VoIP

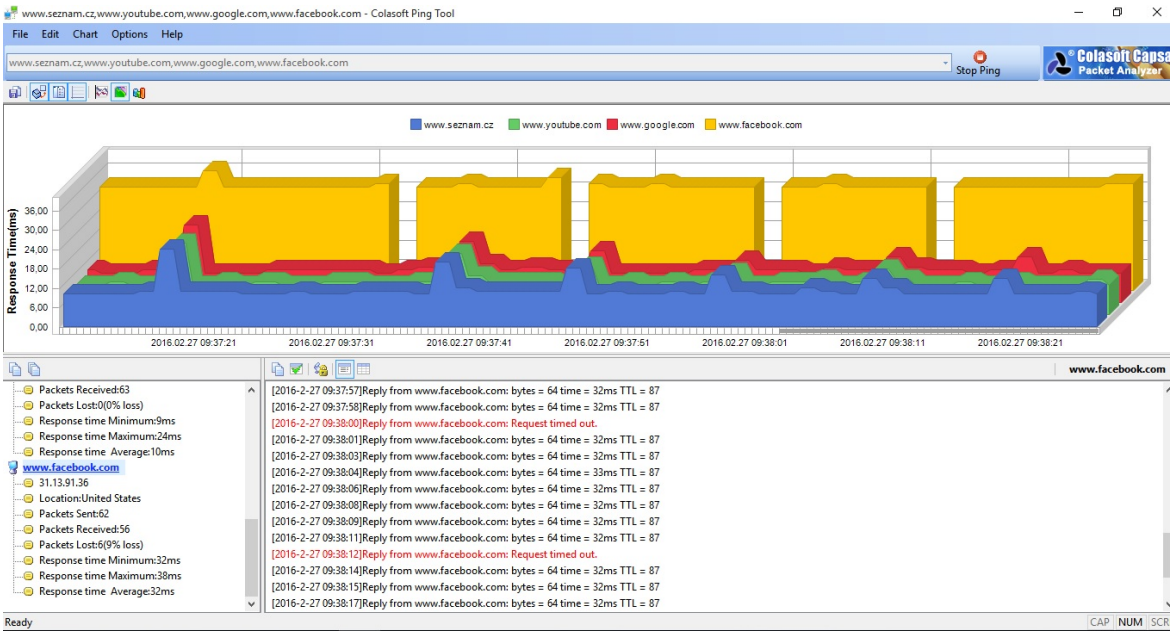
3.2 Colasoft Capsa 8

3.2.1 Nástroje analyzátoru a jejich užití

Součástí instalace analyzátoru jsou 4 freware nástroje od firmy Colasoft - viz. Obrázek 3.11. Je možnost stáhnout a nainstalovat tyto nástroje samostatně a jsou nezávislé na samotném analyzátoru.

Obrázek 3.11: Nástroje Colasoft Capsa

- **Colasoft ping tool** v reálném čase zpracovává odezvy na ICMP echo dotazy, jež v jeden okamžik posílá na námi definované servery. Servery definujeme doménovými jmény nebo IP adresami oddělenými čárkou do kolonky vedle tlačítka start ping. Po spuštění jsou výsledky zobrazeny v grafu, což umožňuje lépe porovnávat vzájemně jednotlivé odezvy (viz Obrázek 3.12).

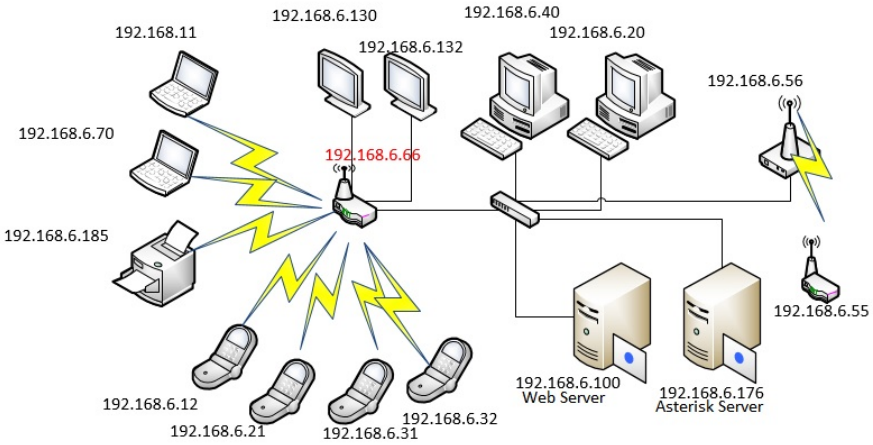


Obrázek 3.12: Graf ICMP odpovědí

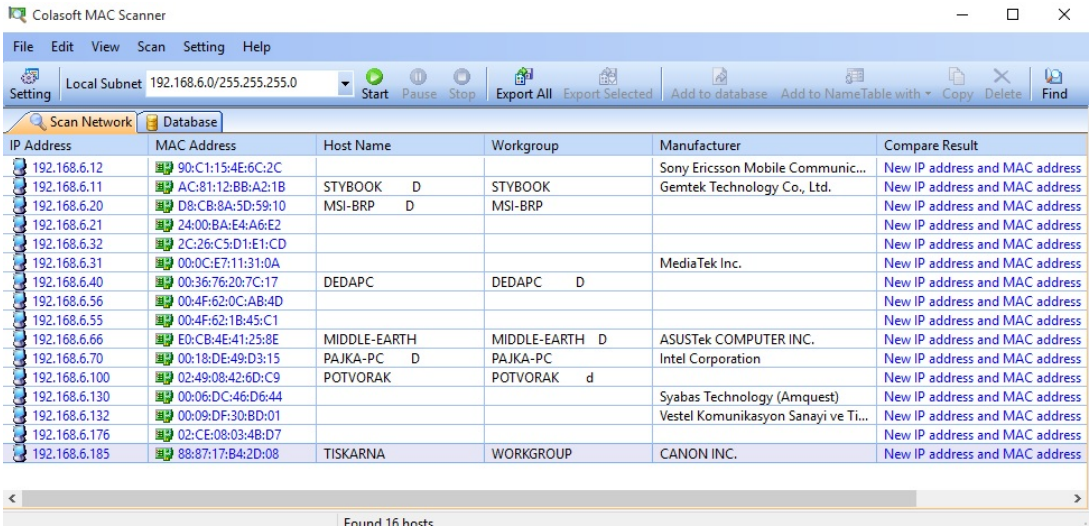
- **Colasoft MAC Scanner**

  je dalším zajímavým nástrojem. Jeho účelem je pomocí ARP dotazů detekovat veškeré aktivní prvky v subnetu, ve němž se nacházíme. Pokud je zařízení aktivní, je k jeho MAC adrese přiřazena IP adresa a v případě dostupnosti i hostname. Některým zařízením přiřadí také značku výrobce. Pokud se výrobce nezobrazuje, není v souboru MAC adres výrobců "oui.dat". Soubor nalezneme v adresáři `C:\ProgramFiles(x86)\ColasoftCapsa8EnterpriseEdition\mui\en_us`. Pokud známe výrobce, v textovém editoru můžeme přidat záznam sami.

  Na Obrázku 3.14 je uveden výpis skenování z topologie (viz Obrázek 3.13).

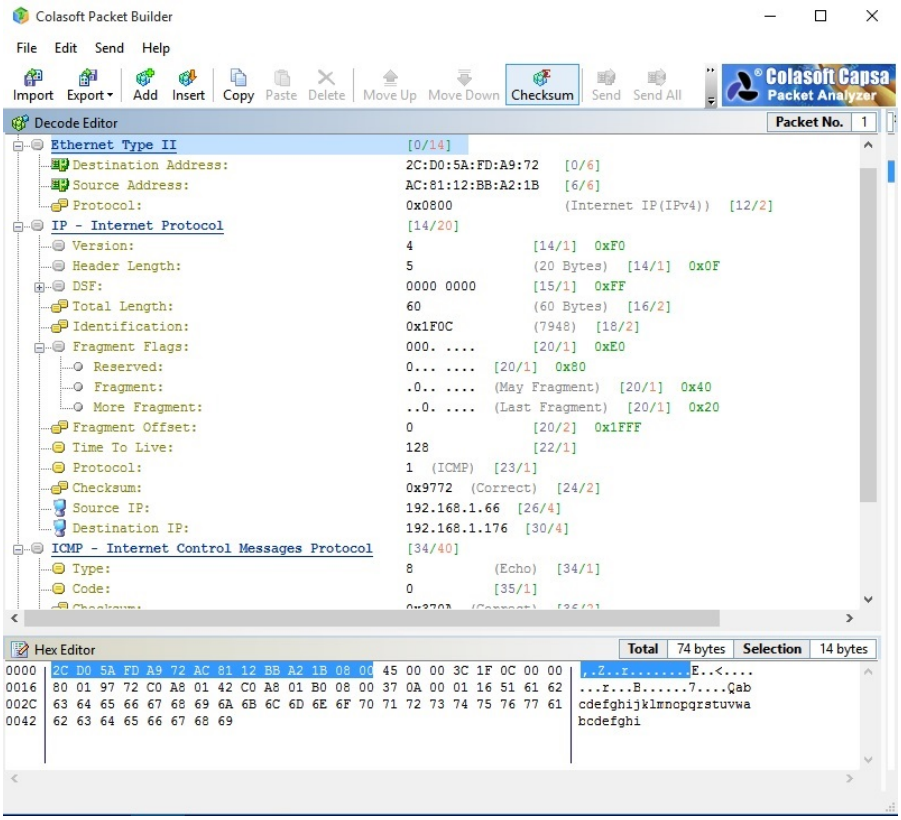


Obrázek 3.13: Topologie skenované sítě



Obrázek 3.14: Výsledek skenování sítě

- **Colasoft Packet Builder** je nástroj, který umožňuje vytvářet pakety nebo upravovat pakety exportované z analyzátoru Capsa. Tím pádem je možné vytvořit pakety s podvrženými adresami nebo namnožit již existující paket, který pak lze využít třeba k útoku na síť. Příklad si uvedeme níže.

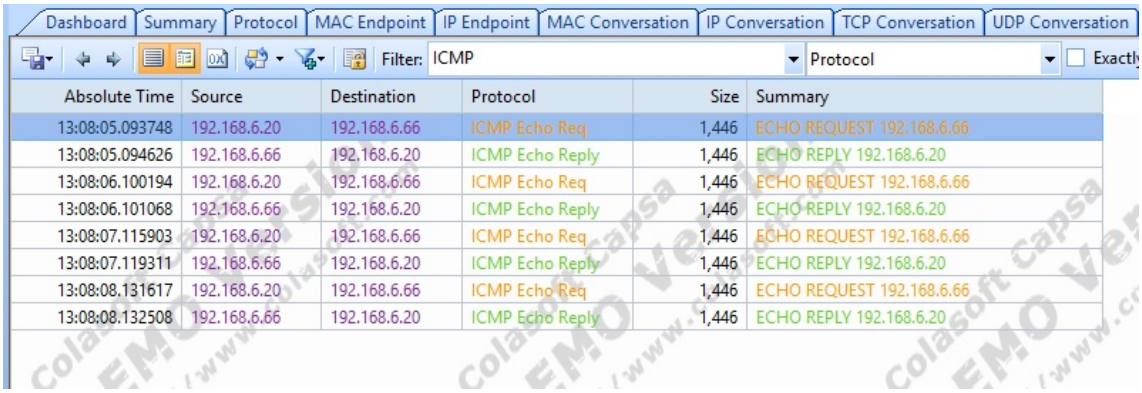


Obrázek 3.15: Vytváření ICMP paketu s podvrženou zdrojovou adresou.

- **Colasoft Packet Player** je nástroj s jehož pomocí můžeme poslat do sítě pakety vytvořené v Packet Builderu. Samozřejmě nemusíme posílat námi vytvořená data, jelikož nástroj zvládne "přehrát"pakety uložené ve formátu .cscpkt, což je výchozí formát pro ukládání zachycených dat v programu Colasoft Capsa. Správnou funkci nástroje lze ověřit kterýmkoli analyzátorem, jež umí odeslaná data znovu zobrazit.

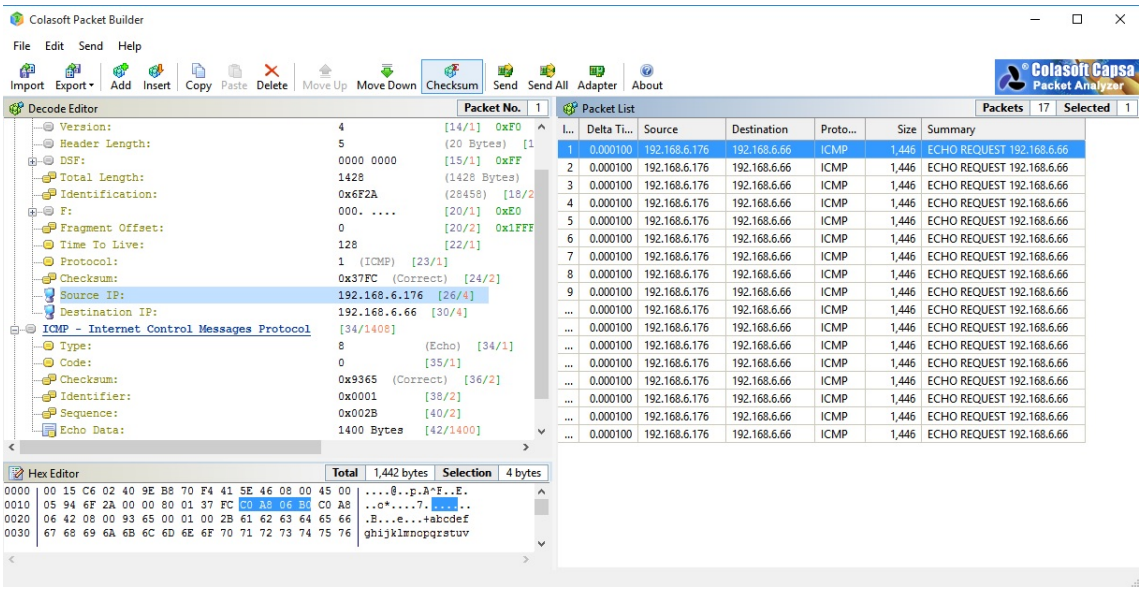
Nyní si předvedeme jak nástroje využít. Spustíme analyzátor a abychom nemuseli tvořit paket od samotného začátku, vytvoříme si paket ICMP, jež odešleme na libovolné zařízení. Spustíme příkazový řádek systému a použijeme příkaz "ping 192.168.6.66 -l 1400", čímž odešleme 5 zpráv ICMP s velikostí 1400 byte. Ty nám po přidání hlaviček narostou o 46 byte. V hlavním okně analyzátoru přepneme na záložku "packet", kde si paket vyfiltrujeme s pravidlem "ICMP Protocol"(viz Obrázek 3.16). Je třeba zastavit zachytávání, jelikož po vypršení limitu zásobníku o data začneme přicházet. Pakety není třeba vytvářet větší, poněvadž po překročení velikosti 1500 byte (MTU ethernetu) je pa-

ket fragmentován. Zařízení, na něž pakety posíláme, čeká s odpovědí, dokud nedostane všechny fragmeny zprávy. Pokud je nedostane, neposílá odpověď. Vytvořit fragmentovanou zprávu je zbytečná komplikace, proto nám rezerva 54 byte neuškodí. Po kliknutí levým tlačítkem vybereme možnost send to packet builder.



Obrázek 3.16: Filtrované ICMP zprávy

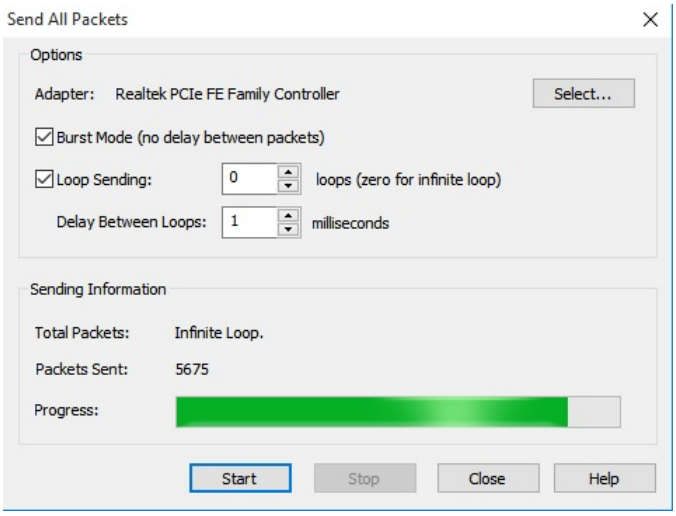
Nyní se nám otevře nástroj packet builder, kde můžeme daný paket upravit. Upravíme tedy informaci Source IP na adresu oběti a pomocí klávesové zkratky ”ctrl + c , ctrl + v”paket namnožíme (viz Obrázek 3.17).



Obrázek 3.17: Úprava a klonování paketu v Packet Builderu

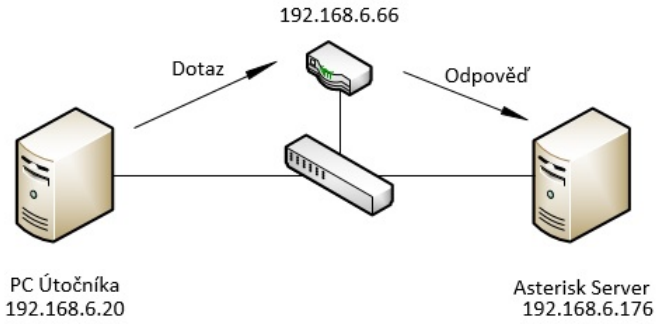
Dále pomocí tlačítka ”Adapter”v horní liště vybereme síťovou kartu, kde chceme pakety odeslat, a tlačítkem ”Send All”přejdeme k nastavení parametrů odesílání. Pakety můžeme odeslat jednou, případně v nekonečné smyčce, můžeme vkládat mezeru mezi

jednotlivé pakety nebo přidáním mezery mezi smyčky odesílat ve vlnách (viz Obrázek 3.18).



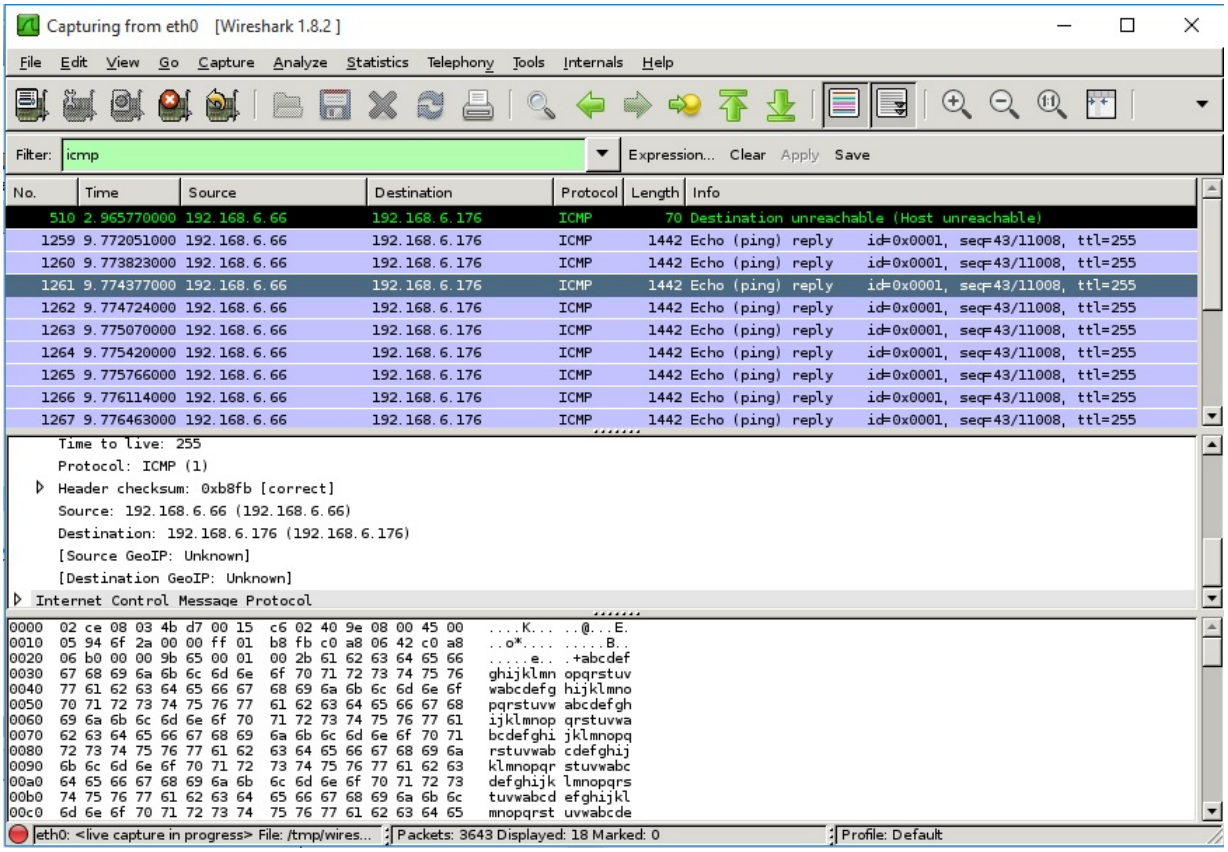
Obrázek 3.18: Nastavení parametrů odesílání paketů

Po spuštění odesílání paketů náš počítač odesílá pakety s podvrženou zdrojovou adresou jiného zařízení. Zařízení, v našem případě směrovač (viz Obrázek 3.19), který náš paket přijme, následně na danou adresu odpoví. Pokud provozu bude nad rámec výkonu směrovače, můžeme router zahltit a zamezit tak komunikaci ostatním uživatelům sítě. Tento útok nazýváme DoS.



Obrázek 3.19: Dos Útok na směrovač/server

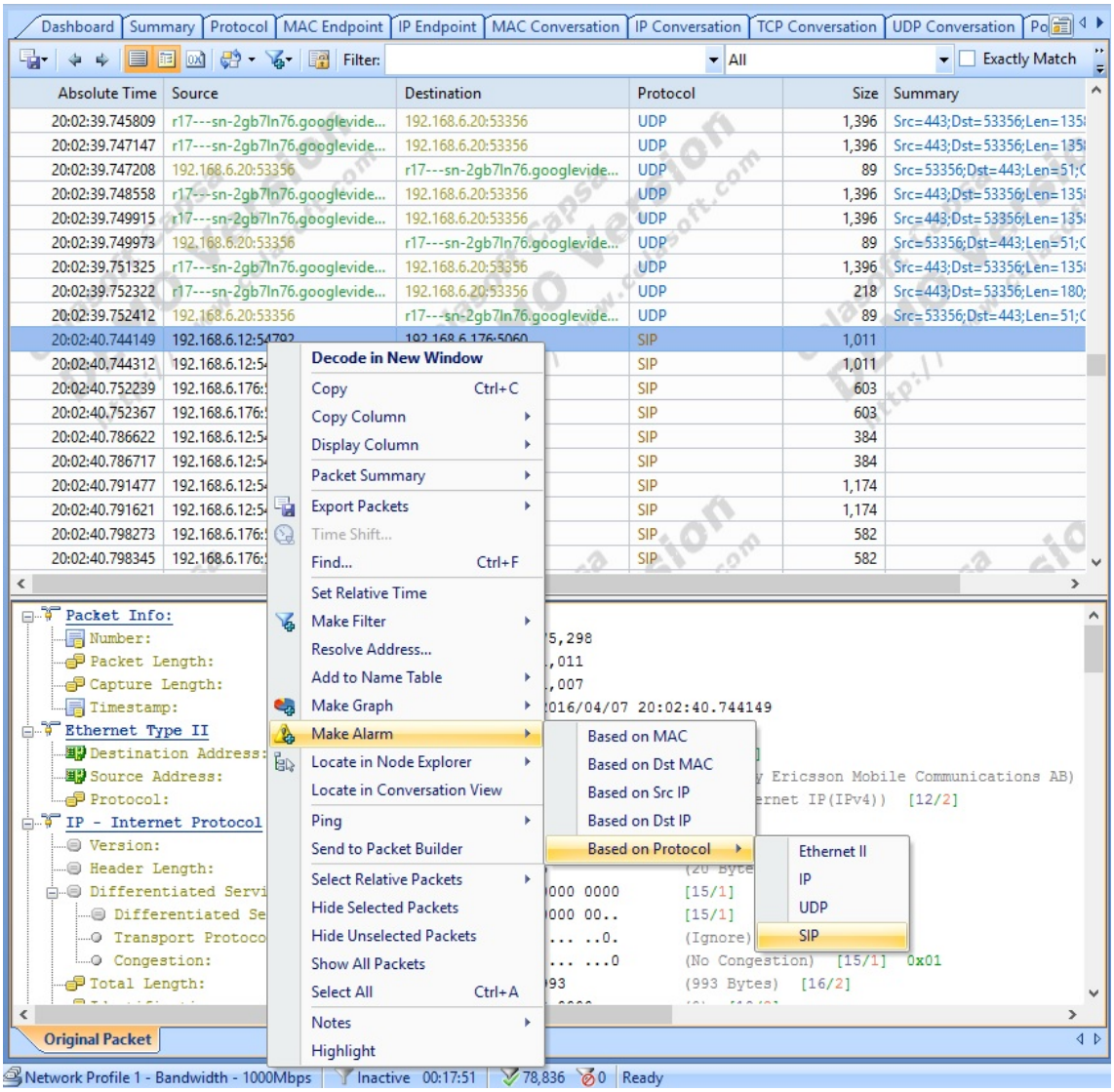
Pro ověření útoku můžeme použít vzdálený wireshark na Asterisk serveru (viz kapitola 3.1.2). Na obrázku 3.20 vidíme uživatelské rozhraní vykreslené v průběhu útoku pomocí Xming serveru na útočícím počítači.



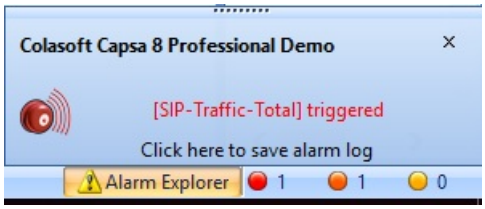
Obrázek 3.20: ICMP odpovědi směrovače

3.2.2 Alarm a Graf

Alarm je funkce, jež nás upozorní na událost v síti. Alarm tvoříme klikem pravého tlačítka myši na určitý paket. Jako první parametr musíme zvolit základ hlídaného parametru (viz Obrázek 3.21), následně nastavujeme spouštěcí podmínky a typ upozornění. Definujeme si např. alarm se základem protokol SIP, spouštěcí podmínka bude počet paketů vyšší než 3/sec. Analyzátor následně sám hlídá tuto situaci v pozorovaných paketech, pokud se objeví signalizace SIP v dané míře, analyzátor nás upozorní (viz Obrázek 3.22).



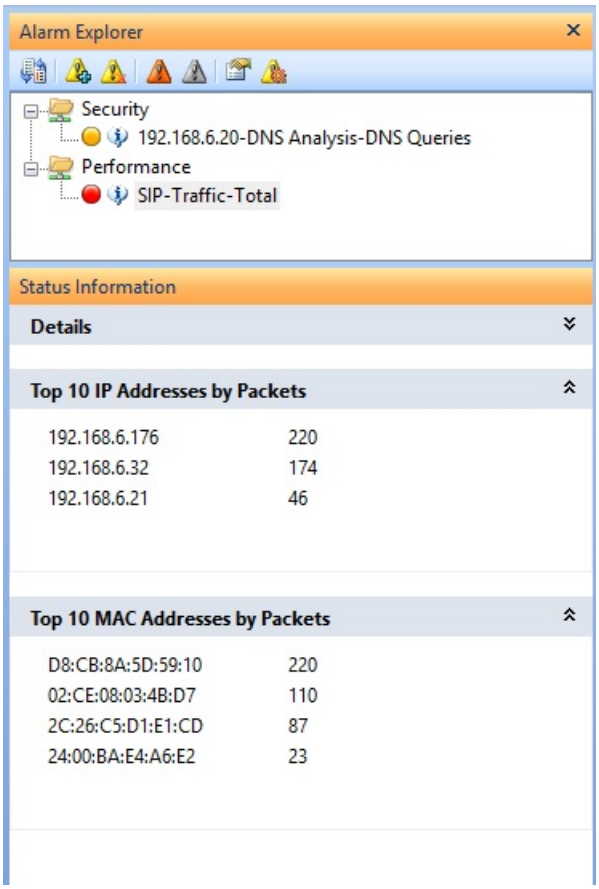
Obrázek 3.21: Možnosti výběru základu alarmu



Obrázek 3.22: Upozornění na SIP provoz

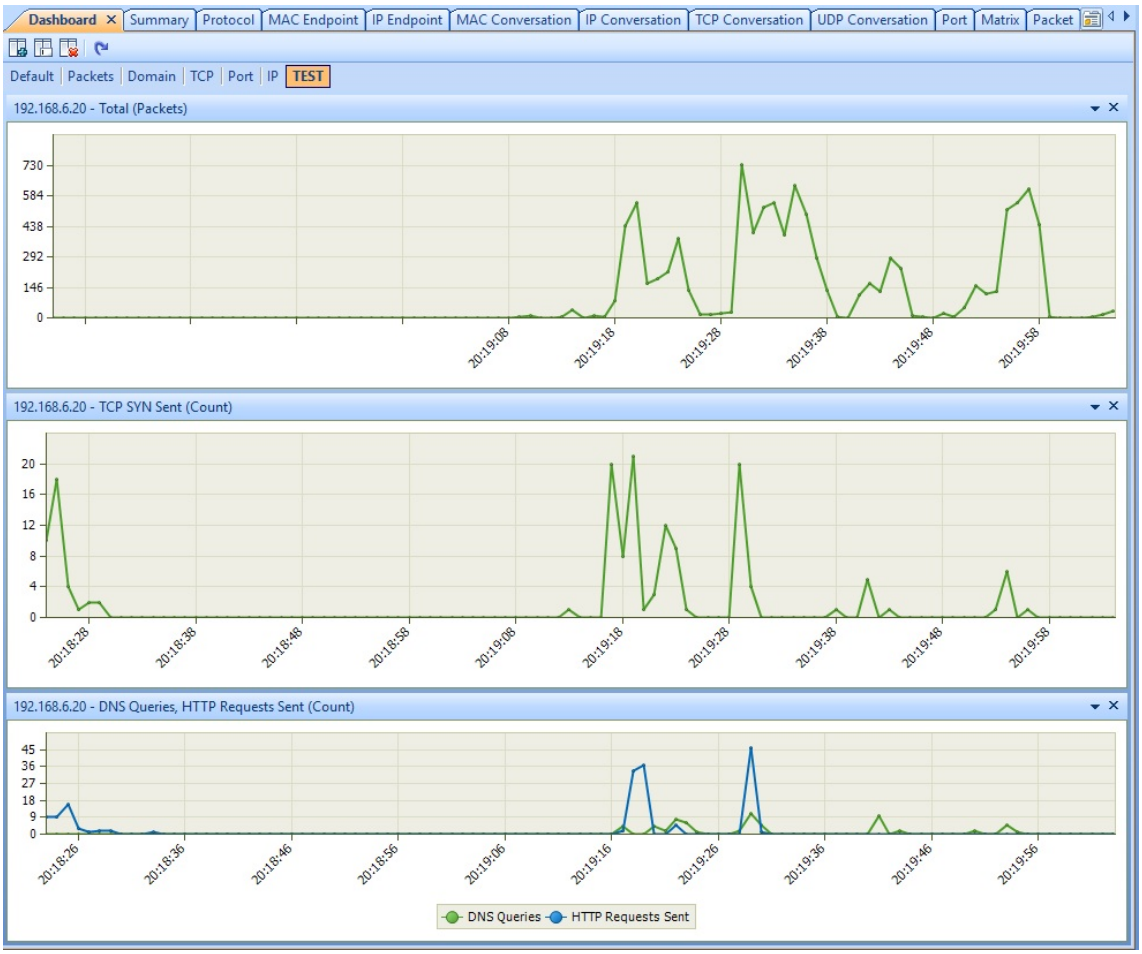
Alarm explorer slouží k procházení úprav alarmů a vyhodnocení výsledků dané situace. Současně si můžeme nastavit, jaké informace chceme zahrnout k výsledkům

daného upozornění. Na obrázku 3.23 můžeme vidět informace vyhodnocené v našem alamu SIP.



Obrázek 3.23: Prohlížeč alarmu SIP

Graf v analyzátoru Capsa vytvoříme obdobně jako alarm (viz Obrázek 3.21). Grafy zde mají několik základních dělení dle zvoleného základu. Pokud např. zvolíme graf se základem na zdrojové adrese, můžeme dále volit graf popisující provoz (Total, Multicast, Broadcast atd.), graf popisující tok (IP, TCP, UDP konverzace), graf týkající se pouze TCP zpráv (počty TCP SYN, TCP FIN atd.), dále grafy DNS dotazů, SMTP/POP připonení , FTP Upload/Download. Pokud ale zvolíme specifický protokol, např. UDP, lze vytvořit graf pouze na přenesená data a počet paketů určité velikosti. Grafy následně nalezneme v záložce "Dashboard"v hlavním okně analyzátoru (viz Obrázek 3.24).



Obrázek 3.24: Graf počtu paketů/s, Graf počtu TCP SYN/s, Graf DNS dotazů/HTTP dotazů

4 Srovnání analyzátorů

1. **Uživatelské rozhraní**

   Jako nejléle zpracovaný analyzátor hodnotím analyzátor Colasoft Capsa. Ovládací prvky jsou jednoduché, orientace v programu je intuitivní a uživatel si na program velice rychle zvykne. Protokoly jsou barevně odlišeny, což zlepšuje orientaci v paketech. Jako zápor uživatelského rozhraní vytýkám využití nekontrastních barev zdojových a cílových adres aktuálně zachycených paketů.

   Druhý v pořadí hodnotím analyzátor Wireshark. Progam je na ovládání velice jednoduchý, a intuitivně najdeme co potřebujeme. Protokoly jsou od sebe barevně odlišeny a, na rozdíl od analyzátoru Capsa, dostatečně kontrastní, tudíž je v nich příjemná orientace.

   Třetí v pořadí umisťuji analyzátor BitShark. Jakožto obdoba wiresharku pro Android se aplikace velice povedla. Ovládání je také velice intuitivní. Barevné zpracování analyzátoru hodnotím jako nejlepší ze všech analyzátorů. Na displeji telefonu nezpůsobuje přílišné přesvětlení displeje a barvy jsou na poled příjemné.

   Jako předposlední analyzátor hodnotím Microsoft Network Monitor. Analyzátor je laděn do 3 odstínů šedé barvy. V základním nastavení nejsou pakety vůbec barevně odděleny a jedná se pouze o seznam na bílém pozadí. Pokud chceme pakety barevně oddělit, je potřeba si pravidla definovat samostatně.

   Posledním analyzátorem v této kategorii je TCPDUMP bez jakéhokoli grafického rozhraní a funguje pouze v příkazové řádce.

2. **Podpora operačních systémů** V hodnocení podle podpory operačního systému se nejlépe umístí TCPDUMP, který není téměř omezen na operační systém. Následuje Wireshark, který je podporován na Linuxu i na Windowsu. Následují analyzátory pro jeden operační systém: Microsoft Network Monitor, Colasoft Capsa, BitShark.

3. **Složitost používání** Dle složitosti analyzátory řadím následovně: Nejjednodužší analyzátor hodnotím Microsoft Network Monitor - má veškeré důležité ovládací prvky analyzátoru v jednom okně. Ovládacích prvků a možností analyzátoru není mnoho, proto tento analyzátor udávám na první místo.

   Na druhé místo udávám BitShark. Jak již bylo zmíněno, ovládání je velice intuitivní a dobře zpracované. Možností není příliž mnoho a pracovat s tímto analyzátorem zvládne i nezkušený analytik.

   Na další příčku umisťuji Wireshark. Ten je sice ovládáním poměrně jednoduchý, ale množstvím možností, nastavení a ovládacích prvků předčí předchozí analyzátory.

   Dále hodnotím analyzátor Colasoft Capsa. Ovládání je také intuitivní, ale množsvím záložek a množstvím variací nastavení analyzátor předčil své soupeře. Zároveň bych ho ale umístil na první místo za kvalitu zpracování velkého množství vlastností s tak uživatelsky přívětivým výsledkem.

Jako poslední analyzátor je TCPDUMP. Možností a vlastností analyzátoru sice není mnoho, ale pro nového uživatele tohoto analyzátoru je používání téměř nemožné bez pomoci manuálu k programu.

4. **Náklady** Z hlediska nákladů je nejlepší analyzátor TCPDUMP a Microsoft Network Monitor, neboť zdarma umožňují veškeré své funkce. Následuje BitShark, za nějž zaplatíme jednorázově poměrně malou částku. Wireshark zdarma poskytuje také mnoho funkcí, nicméně analýza bezdrátu pomocí Wiresharku je bez užití NDIS ovladačů nákladná na rozdíl od MNM, kde je funkce analýzy 802.11 zdarma. Nejdražším analyzátorem je Colasoft Capsa. Ve free verzi poskytuje pouze funkce týkající se živého zachytávání, které je omezeno na pouhých 8 MB dat. Trial licence Profesional a Enterprice verze posunují limity funkcí a množství zachycených dat, ale jsou omezeny na 15 dní a není umožněn export výsledků. Pro regulérní používání tohoto analyzátoru v ethernetové síti tedy potřebujeme minimálně licenci na verzi Profesional za 695$ ročně.

5 Závěr

Pokud potřebujeme kvalitní a pohodlnou analýzu a nehledíme na náklady, analyzátor Colasoft Capsa je pro nás nejlepší volba. Tabulky výsledků analýzy jsou přehledné, dobře graficky zpracované a funkci report využijeme při tvorbě protokolu o stavu provozu sítě.

Analyzátor Wireshark obhájil svou hodnost nejpoužívanějšího analyzátoru. Nejen jeho dostupnost i pro Linux i pro Windows rozšiřuje portfolio uživatelů, ale také množství funkcí, grafické provedení a jednoduchost jeho použití posouvají tento analyzátor na první příčku. Uživatelská komunita a podpora tohoto programu s množstvím návodů a uživatelských modulů se nedá s jinými analyzátory srovnávat, proto zdaleka nelze popsat všechny možnosti, kterými daný analyzátor disponuje.

Microsoft Network Monitor je schopen analyzovat síťový provoz v promiskuitním režimu a sloužit jako analyzátor veškerého síťového provozu. Ale jeho přednost je ve schopnosti přiřazení aplikace k jednotlivým komuminakčím streamům. Tudíž je to výborný analyzátor pro analýzu provozu generovaného neznámým programem. MNM je také výborný v analýze bezdrátového provozu 802.11, jenž je podporován bez přídavných modulů, karet či ovladačů.

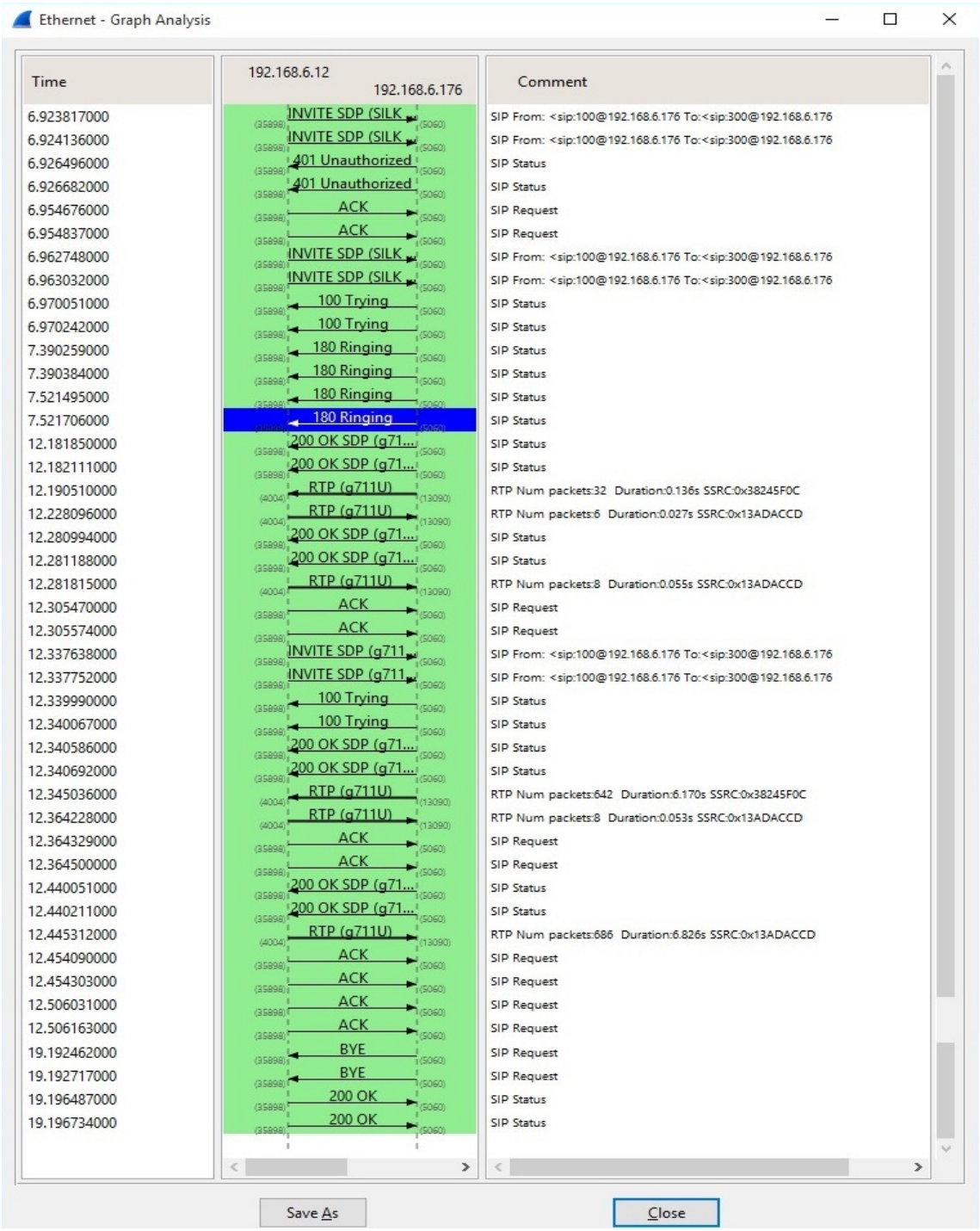
TCPDUMP je analyzátor pro velice pokročilé uživatele používaný hlavně tam, kde má analytik pouze SSH přístup. Neposkytuje však možnost globálního přehledu o provozu. Je schopen pouze dekódovat pakety a zobrazit obsah uživateli.

Bitshark je plnohodnotný analyzátor, ale z principu zachytávání dat v síti s ním není možno zachytávat všechna data, ale pouze komunikaci daného mobilního telefonu s bezdrátovou sítí. Pro tuto analýzu je ale tento analyzátor špičkou mezi analyzátory pro Android.

Literatura

1. COLASOFT. *Colasoft Capsa 8* [online]. [cit. 2016-04-15]. Dostupný z WWW: ⟨http://www.colasoft.com/capsa-free/⟩.
2. COLASOFT. *Colasoft Capsa 8 Enterprise Trial*. Dostupný z WWW: ⟨http://www.colasoft.com/capsa-free/⟩.
3. COMBS, Gerald. *Wireshark* [online]. [cit. 2016-04-15]. Dostupný z WWW: ⟨https://www.wireshark.org/#download⟩.
4. HAMILTON, Blake. *BitShark* [online]. [cit. 2016-04-15]. Dostupný z WWW: ⟨https://play.google.com/store/apps/details?id=blake.hamilton.bitshark&hl=en⟩.
5. HARRISON, Colin. *Xming X Server* [online]. [cit. 2016-04-15]. Dostupný z WWW: ⟨http://www.straightrunning.com/XmingNotes/⟩.
6. HARRISON, Colin. *Xming X Server 6.9.0.31* [online]. [cit. 2016-04-15]. Dostupný z WWW: ⟨https://sourceforge.net/projects/xming/files/Xming/6.9.0.31/⟩.
7. MICROSOFT. *Microsoft Network Monitor 3.4* [online]. [cit. 2016-04-15]. Dostupný z WWW: ⟨https://www.microsoft.com/en-us/download/details.aspx?id=4865⟩.
8. REVERBED-TECHNOLOGY. *WinDump* [online]. [cit. 2016-04-15]. Dostupný z WWW: ⟨https://www.winpcap.org/windump/install/default.htm⟩.
9. RIVERBED-TECHNOLOGY. *AirPcap* [online]. [cit. 2016-04-15]. Dostupný z WWW: ⟨http://www.cacetech.com/products/catalog/index.php⟩.
10. RIVERBED-TECHNOLOGY. *WinPcap* [online]. [cit. 2016-04-15]. Dostupný z WWW: ⟨https://www.winpcap.org/install/⟩.
11. SANDERS, Chris. *Analýza sítí a řešení problémů v programu Wireshark*. Brno: Computer Press, 2012. ISBN 978-80-251-3718-5.
12. SL, Tarlogic Security. *Acrylic Wifi Compatible monitor mode Wi-Fi cards under windows* [online]. [cit. 2016-04-15]. Dostupný z WWW: ⟨https://www.acrylicwifi.com/en/support/compatible-hardware/⟩.
13. SL, Tarlogic Security. *Acrylic Wifi Profesional* [online]. [cit. 2016-04-15]. Dostupný z WWW: ⟨https://www.acrylicwifi.com/en/wlan-software/wifi-analyzer-acrylic-professional/⟩.
14. TATHAM, Simon. *Putty* [online]. [cit. 2016-04-15]. Dostupný z WWW: ⟨http://www.putty.org/⟩.
15. ULF LAMPING Richard Sharpe, Ed Warnicke. *Wireshark User's Guide* [online]. [cit. 2016-04-15]. Dostupný z WWW: ⟨https://www.wireshark.org/docs/wsug_html_chunked/⟩.

A Graf toku VoIP



Obrázek A.1: Posloupnost signalizace SIP